

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-122635
(P2003-122635A)

(43)公開日 平成15年4月25日 (2003.4.25)

(51) Int.Cl.⁷
 G 06 F 12/14
 12/00
 15/00

識別記号
 3 1 0
 5 3 7
 3 3 0

F I
 G 06 F 12/14
 12/00
 15/00

テマコード(参考)
 5 B 0 1 7
 5 B 0 8 2
 5 B 0 8 5

審査請求 未請求 請求項の数27 OL (全 26 頁)

(21)出願番号 特願2002-221630(P2002-221630)
 (22)出願日 平成14年7月30日 (2002.7.30)
 (31)優先権主張番号 特願2001-236030(P2001-236030)
 (32)優先日 平成13年8月3日 (2001.8.3)
 (33)優先権主張国 日本 (JP)

(71)出願人 000005821
 松下電器産業株式会社
 大阪府門真市大字門真1006番地
 (72)発明者 山本 雅哉
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (72)発明者 岡本 隆一
 大阪府門真市大字門真1006番地 松下電器
 産業株式会社内
 (74)代理人 100098291
 弁理士 小笠原 史朗

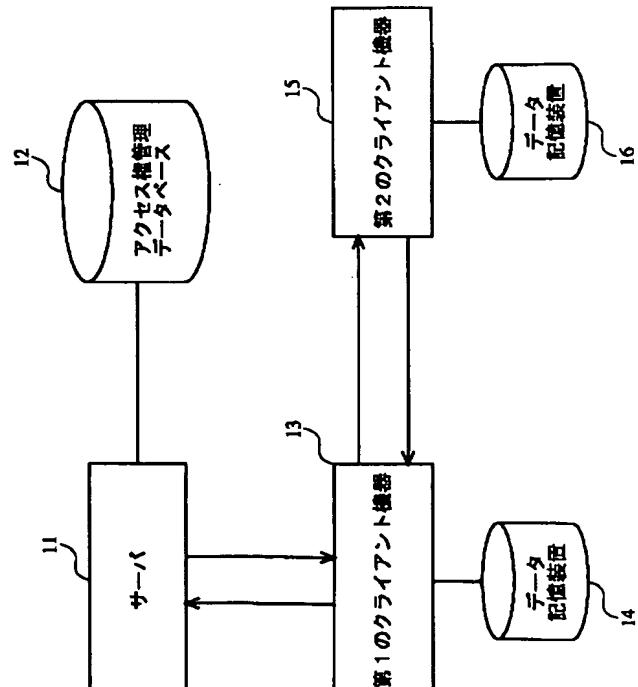
最終頁に続く

(54)【発明の名称】 アクセス権制御システム

(57)【要約】

【課題】 ピアツーピア型のファイル交換システムにおけるクライアント機器において、所望のアクセス権制御が可能なアクセス権制御システムを提供する。

【解決手段】 アクセス権制御システムは、サーバ1、アクセス権管理データベース12、第1および第2のクライアント機器13および15、データ記憶装置14および16を備えている。第1および第2のクライアント機器13および15は、ピアツーピア型のファイル交換システムを共有する。第1および第2のクライアント機器13および15は、サーバ11に対してアクセス可能に構成されている。アクセス権管理データベース12は、アクセス権管理リストを格納する。第1のクライアント機器13は、第2のクライアント機器15からデータの要求された場合、サーバ11にそのアクセス権を問い合わせ、サーバ11によってそのアクセス権がアクセス権管理リストを用いて判定される。



【特許請求の範囲】

【請求項1】 エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を判断するためのアクセス権制御システムであって、

前記クライアント機器と通信可能に接続され、前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するサーバを備え、

前記サーバは、前記アクセス権の問い合わせに対して前記アクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を返信するアクセス可否判定部を含み、

前記クライアント機器は、

他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記アクセス可否判定部に問い合わせるアクセス可否問い合わせ部と、

前記アクセス可否問い合わせ部によって問い合わせた結果、前記アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを他の機器に対して直接的に送信するデータ送信部とを含む、アクセス権管理システム。

【請求項2】 前記サーバが管理するアクセス権管理リストには、それぞれの前記クライアント機器が管理するデータ毎にアクセス可能な機器を示す前記アクセス権が記述され、

前記アクセス可否問い合わせ部は、前記データ送信を要求されたデータ毎に、前記アクセス可否判定部に問い合わせを行い、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果を返信する、請求項1に記載のアクセス権管理システム。

【請求項3】 さらに、前記サーバが管理するアクセス権管理リストには、アクセス可能な時間を示す時間条件が前記データ毎に記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部から問い合わせされた現在時刻に応じて前記時間条件を参照して、前記データ毎にそのアクセス権を判断する、請求項2に記載のアクセス権管理システム。

【請求項4】 さらに、前記サーバが管理するアクセス権管理リストには、アクセス可能な回数を示す回数条件が前記データ毎に記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部から問い合わせされた回数に応じて前記回数条件を参照して、前記データ毎にそのアクセス権を判断する、請求項2に記載のアクセス権管理システム。

【請求項5】 さらに、前記サーバが管理するアクセス権管理リストには、前記データ毎に提供された当該データの複製に関する制限を示す複製条件が記述され、

前記データ毎の問い合わせに応じて、そのアクセス権を判断し判断結果と共に前記複製条件を返信し、前記データ送信部は、前記アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを前記複製条件を付加して他の機器に対して直接的に送信する、請求項2に記載のアクセス権管理システム。

【請求項6】 前記サーバは、他のプロキシを介して前記クライアント機器と通信可能に接続されていることを特徴とする、請求項1に記載のアクセス権管理システム。

【請求項7】 前記アクセス可否問い合わせ部は、他の機器からデータ送信を要求され、その要求に対する前記アクセス権を前記アクセス可否判定部に問い合わせるとときに、前記クライアント機器であることを証明するための第1の証明書と当該他の機器を証明するための第2の証明書とを付加して前記アクセス可否判定部に問い合わせ、

前記アクセス可否判定部は、前記第1および第2の証明書を用いて前記アクセス可否問い合わせ部からの問い合わせを認証した後、前記アクセス権を判断し判断結果を返信する、請求項1に記載のアクセス権管理システム。

【請求項8】 前記証明書にはX. 509を使用することを特徴とする、請求項7記載のアクセス権制御システム。

【請求項9】 エンドユーザが所有する第1のクライアント機器に対して、第2のクライアント機器が直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を判断するためのアクセス権制御システムであって、

少なくとも前記第2のクライアント機器と通信可能に接続され、少なくとも前記第1および第2のクライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するサーバを備え、

前記サーバは、前記アクセス権の問い合わせに対して前記アクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を返信するアクセス可否判定部を含み、

前記第2のクライアント機器は、

前記第1のクライアント機器に対して直接的なデータ送信を要求する際に、その要求に対する前記アクセス権を前記アクセス可否判定部に問い合わせるアクセス可否問い合わせ部と、

前記アクセス可否問い合わせ部によって問い合わせた結果、前記アクセス可否判定部から返信された判断結果がアクセス可の場合、前記第1のクライアント機器に対して当該判断結果を付加して前記直接的なデータ送信を要求するデータ要求部とを含み、

前記第1のクライアント機器は、前記データ要求部から送信された前記判断結果がアクセス可の場合、前記データ要求部に該当するデータを直接的に送信する、

ト機器に対して直接的に送信するデータ送信部を含み、前記第2のクライアント機器は、さらに前記データ要求部からの要求に応じて前記データ送信部から送信されたデータを直接的に受信するデータ受信部とを含む、アクセス権管理システム。

【請求項10】 前記サーバが管理するアクセス権管理リストには、それぞれの前記クライアント機器が管理するデータ毎にアクセス可能な機器を示す前記アクセス権が記述され、

前記アクセス可否問い合わせ部は、前記データ送信を要求するデータ毎に、前記アクセス可否判定部に問い合わせを行い、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果を返信する、請求項9に記載のアクセス権管理システム。

【請求項11】 さらに、前記サーバが管理するアクセス権管理リストには、アクセス可能な時間を示す時間条件が前記データ毎に記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部から問い合わせされた現在時刻に応じて前記時間条件を参照して、前記データ毎にそのアクセス権を判断する、請求項10に記載のアクセス権管理システム。

【請求項12】 さらに、前記サーバが管理するアクセス権管理リストには、アクセス可能な回数を示す回数条件が前記データ毎に記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部から問い合わせされた回数に応じて前記回数条件を参照して、前記データ毎にそのアクセス権を判断する、請求項10に記載のアクセス権管理システム。

【請求項13】 さらに、前記サーバが管理するアクセス権管理リストには、前記データ毎に提供された当該データの複製に関する制限を示す複製条件が記述され、

前記アクセス可否判定部は、前記アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果と共に前記複製条件を返信し、

前記データ要求部は、前記アクセス可否判定部から返信された判断結果がアクセス可の場合、前記第1のクライアント機器に対して前記判断結果および前記複製条件と共に前記直接的なデータ送信を要求し、

前記データ送信部は、前記データ要求部から送信された前記判断結果がアクセス可の場合、前記データ要求部から要求されたデータと共に前記複製条件を前記データ受信部に対して直接的に送信し、

前記データ受信部は、前記データ送信部から送信されたデータを直接的に受信し、そのデータが前記複製条件によってその後の複製が制限される、請求項10に記載のアクセス権管理システム。

【請求項14】 前記サーバは、他のプロキシを介して

ることを特徴とする、請求項9に記載のアクセス権管理システム。

【請求項15】 前記アクセス可否問い合わせ部は、前記第1のクライアント機器に対してデータ送信を要求するに、その要求に対する前記アクセス権を前記アクセス可否判定部に問い合わせるときに、前記第2のクライアント機器であることを証明するための証明書を付加して前記アクセス可否判定部に問い合わせ、

前記アクセス可否判定部は、前記証明書を用いて前記アクセス可否問い合わせ部からの問い合わせを認証した後、前記アクセス権を判断し判断結果を返信する、請求項9に記載のアクセス権管理システム。

【請求項16】 さらに、前記アクセス可否判定部は、前記判断結果に前記サーバの判断であることを証明するための署名を付加して返信し、

前記データ要求部は、前記アクセス可否判定部から返信された判断結果がアクセス可の場合、前記第1のクライアント機器に対して前記署名が付加された判断結果および前記証明書と共に前記直接的なデータ送信を要求し、前記データ送信部は、前記データ要求部から送信された前記判断結果の署名を用いて認証を行い当該判断結果がアクセス可の場合、前記データ要求部から要求されたデータと共に前記複製条件を前記データ受信部に対して直接的に送信する、請求項15に記載のアクセス権管理システム。

【請求項17】 前記証明書にはX. 509を使用することを特徴とする、請求項15記載のアクセス権制御システム。

【請求項18】 エンドユーザが所有する複数のクライアント機器同士で当該クライアント機器が管理するデータを直接的に送受信を行う際に、そのアクセス可否を示すアクセス権を判断するサーバであって、

前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理部と、前記クライアント機器から送信される前記アクセス権の問い合わせに対して、前記アクセス権管理部において前記アクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を問い合わせたクライアント機器に対して返信するアクセス可否判定部を含む、サーバ。

【請求項19】 他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎に前記アクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるエンドユーザが所有するクライアント機器であって、

他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記サーバに問い合わせるアクセス可否問い合わせ部と、

前記アクセス可否問い合わせ部によって問い合わせた結果

場合、他の機器の要求に応じて直接的に前記データ送信を行うデータ送信部とを含む、クライアント機器。

【請求項 2 0】 他の機器に直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を、機器毎に前記アクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるエンドユーザが所有するクライアント機器であって、他の機器に直接的なデータ送信を要求する際に、その要求に対する前記アクセス権を前記サーバに問い合わせるアクセス可否問い合わせ部と、

前記アクセス可否問い合わせ部によって問い合わせた結果、前記サーバから返信された判断結果がアクセス可の場合、他の機器に対して当該判断結果を付加して前記直接的なデータ送信を要求するデータ要求部とを含む、クライアント機器。

【請求項 2 1】 他の機器から要求されることによって直接的なデータ送信を行うエンドユーザが所有するクライアント機器であって、

他の機器からの前記直接的なデータ送信の要求とその要求に付加されて送信される当該データ送信に対するアクセス可否を示すアクセス権の判断結果とを受信する受信部と、

前記受信部で受信した前記判断結果がアクセス可の場合、他の機器から要求されたデータを直接的に送信するデータ送信部とを含む、クライアント機器。

【請求項 2 2】 前記判断結果には、前記アクセス権の判断をした機器であることを証明するための署名が付加されており、

前記データ送信部は、前記判断結果の署名に対する認証を行うことによって当該判断結果の正当性を評価し、当該判断結果が正当かつアクセス可の場合、他の機器から要求されたデータを直接的に送信する、請求項 2 1 に記載のクライアント機器。

【請求項 2 3】 エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断するためのアクセス権制御方法であって、

前記サーバにおいて、前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、

前記クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記クライアント機器から前記サーバに問い合わせるアクセス可否問い合わせステップと、

前記アクセス可否問い合わせステップによる問い合わせに対して、前記アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権を前記サーバで判断し判断結果を前記クライ

前記アクセス可否判定ステップによって返信された判断結果がアクセス可の場合、要求されたデータを前記クライアント機器から他の機器に対して直接的に送信するデータ送信ステップとを含む、アクセス権制御方法。

【請求項 2 4】 エンドユーザが所有する第1のクライアント機器に対して、第2のクライアント機器が直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を当該第2のクライアント機器と通信可能に接続されたサーバで判断するためのアクセス権制御方法であって、

前記サーバにおいて、少なくとも前記第1および第2のクライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、前記第2のクライアント機器が前記第1のクライアント機器に直接的なデータ送信を要求する際に、その要求に対する前記アクセス権を前記第2のクライアント機器から前記サーバに問い合わせるアクセス可否問い合わせステップと、

前記アクセス可否問い合わせステップによる問い合わせに対して、前記アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権を前記サーバで判断し判断結果を前記第2のクライアント機器に返信するアクセス可否判定ステップと、

前記アクセス可否判定ステップから返信された判断結果がアクセス可の場合、前記第1のクライアント機器に対して前記判断結果を付加して前記直接的なデータ送信を要求するデータ要求ステップと、

前記データ要求ステップによって送信された前記判断結果がアクセス可の場合、前記データ要求ステップによって要求されたデータを前記第2のクライアント機器に対して直接的に送信するデータ送信ステップと、

前記データ送信ステップによって前記第1のクライアント機器から送信されたデータを前記第2のクライアント機器で直接的に受信するデータ受信ステップとを含む、アクセス権制御方法。

【請求項 2 5】 エンドユーザが所有するクライアント機器同士で当該クライアント機器が管理するデータを直接的に送受信を行う際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断させるためのアクセス権制御プログラムを記録した当該サーバが読み取り可能な記録媒体であつて、

前記クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、

前記クライアント機器がデータの直接的な送受信を行う際に、当該クライアント機器から前記サーバに対して行われるその送受信に対する前記アクセス権の問い合わせ

るアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を当該クライアント機器に返信するアクセス可否判定ステップとを含む、アクセス権制御プログラムを記録した記録媒体。

【請求項26】他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎に前記アクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるアクセス権制御プログラムを記録したエンドユーザが所有するクライアント機器が読み取り可能な記録媒体であって、前記クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対する前記アクセス権を前記サーバに問い合わせるアクセス可否問い合わせステップと、前記アクセス可否問い合わせステップによって問い合わせた結果、前記サーバから返信された判断結果がアクセス可の場合、要求されたデータを前記クライアント機器から他の機器に対して直接的に送信するデータ送信ステップとを含む、アクセス権制御プログラムを記録した記録媒体。

【請求項27】他の機器に直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を、機器毎に前記アクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるアクセス権制御プログラムを記録したエンドユーザが所有するクライアント機器が読み取り可能な記録媒体であって、他の機器に直接的なデータ送信を要求する際に、その要求に対する前記アクセス権を前記サーバに問い合わせるアクセス可否問い合わせステップと、前記アクセス可否問い合わせステップによって問い合わせた結果、前記サーバから返信された判断結果がアクセス可の場合、他の機器に対して当該判断結果を附加して前記直接的なデータ送信を要求するデータ要求ステップとを含む、アクセス権制御プログラムを記録した記録媒体。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、ネットワークにおいてピアツーピア形式でデータ交換を行う際のアクセス権制御システムに関する。

【0002】

【従来の技術】近年、ピアツーピアコンピューティングが注目を集めている。ピアツーピアコンピューティングとは、ネットワークで接続された機器同士で直接やり取りしあうことにより、コンピュータリソース（CPUパワーやハードディスクのスペース）や各種サービス（メッセージやファイル交換システムなど）を共有することができ、機器同士の共同作業さえも可能となる技術である。このピアツーピア型のファイル交換システムでは、

で直接的な通信を行い、当該機器が管理しているファイルを交換することが可能である。

【0003】上記ピアツーピア型のファイル交換システムにおけるクライアント機器が管理するファイルに対する他からのアクセスの可否（以下、アクセス権と記載する）は、当該クライアント機器自身によって行われる。例えば、アクセス先（データの提供元）のクライアント機器では、アクセス元（データの提供先）のクライアント機器に対してパスワードを要求し、正しいパスワードがアクセス元のクライアント機器から送信された場合のみ、アクセス先のクライアント機器が管理するファイルに対するアクセスを許可するといったアクセス権の制御が行われる。さらに、アクセス先のクライアント機器が行う複雑なアクセス権制御としては、アクセス日時やアクセス元のクライアント機器を識別する識別子によるアクセス権制御があり、さらにアクセス先のクライアント機器が管理する各ファイル毎に、それぞれ固有の制御情報を設定するものなどが考えられる。

【0004】

【発明が解決しようとする課題】このような複雑なアクセス権制御は、アクセス先のクライアント機器が処理能力の高いパーソナルコンピュータ等で構成されている場合、実現することは容易である。しかしながら、アクセス先のクライアント機器が処理能力の限られた民生機器で構成されている場合、上述したような複雑なアクセス権制御を実現することは非常に困難である。また、パーソナルコンピュータとは異なり、処理能力の限られた民生機器においては、購入後にその内部に格納されたソフトウェアを交換することは非常に困難であり、上述したアクセス権制御の方法を後から追加あるいは変更することは不可能である。

【0005】一方、上記ピアツーピア型のファイル交換システムと通信可能に接続されたサーバに、当該システム内に設けられたクライアント機器がそれぞれ管理するファイルを、リストとして管理することも行われている。このサーバで管理されているリストは、上記クライアント機器が管理しているファイル名称とそのクライアント機器が記述されており、同じシステム内に設けられたクライアント機器が当該リストを参照することによって、所望のファイルの有無およびそれを管理しているクライアント機器が判明するようになっている。しかしながら、上記サーバにおいては、上述したアクセス権制御を行う機能は有しておらず、最終的には、所望のファイルを管理しているアクセス先のクライアント機器自身によって上述と同様のアクセス権制御が行われている。

【0006】それ故に、本発明の目的は、ピアツーピア型のファイル交換システムにおけるクライアント機器において、所望のアクセス権制御が実行可能なアクセス権制御システムを提供することである。

◆◆◆◆◆

【課題を解決するための手段および発明の効果】上記目的を達成するために、本発明は、以下に述べるような特徴を有している。第1の発明は、エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を判断するためのアクセス権制御システムであって、クライアント機器と通信可能に接続され、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するサーバを備え、サーバは、アクセス権の問い合わせに対してアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を返信するアクセス可否判定部を含み、クライアント機器は、他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をアクセス可否判定部に問い合わせるアクセス可否問い合わせ部と、アクセス可否問い合わせ部によって問い合わせた結果、アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを他の機器に対して直接的に送信するデータ送信部とを含む。

【0008】第1の発明によれば、データの提供元となるクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0009】第2の発明は、第1の発明に従属する発明であって、サーバが管理するアクセス権管理リストには、それぞれのクライアント機器が管理するデータ毎にアクセス可能な機器を示すアクセス権が記述され、アクセス可否問い合わせ部は、データ送信を要求されたデータ毎に、アクセス可否判定部に問い合わせを行い、アクセス可否判定部は、アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果を返信する。

【0010】第2の発明によれば、それぞれのクライアント機器が管理するデータ毎にアクセス権を設定することが可能となる。

【0011】第3の発明は、第2の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、アクセス可能な時間を示す時間条件がデータ

い合わせ部から問い合わせされた現在時刻に応じて時間条件を参照して、データ毎にそのアクセス権を判断する。

【0012】第3の発明によれば、それぞれのクライアント機器が管理するデータ毎に、そのアクセス可能時間を条件としたアクセス権を設定することが可能となる。

【0013】第4の発明は、第2の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、アクセス可能な回数を示す回数条件がデータ毎に記述され、アクセス可否判定部は、アクセス可否問い合わせ部から問い合わせされた回数に応じて回数条件を参照して、データ毎にそのアクセス権を判断する。

【0014】第4の発明によれば、それぞれのクライアント機器が管理するデータ毎に、そのアクセス可能回数を条件としたアクセス権を設定することが可能となる。

【0015】第5の発明は、第2の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、データ毎に提供された当該データの複製に関する制限を示す複製条件が記述され、アクセス可否判定部は、アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果と共に複製条件を返信し、データ送信部は、アクセス可否判定部から返信された判断結果がアクセス可の場合、要求されたデータを複製条件を付加して他の機器に対して直接的に送信する。

【0016】第5の発明によれば、それぞれのクライアント機器が管理するデータ毎に、データ取得後の複製に関する制限を付加することが可能となる。

【0017】第6の発明は、第1の発明に従属する発明であって、サーバは、他のプロキシを介してクライアント機器と通信可能に接続されていることを特徴とする。

【0018】第6の発明によれば、アクセス権を問い合わせる提供元のクライアント機器がサーバと直接通信が不可能であっても、他のプロキシを介してアクセス権の問い合わせが可能となり、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことができる。

【0019】第7の発明は、第1の発明に従属する発明であって、アクセス可否問い合わせ部は、他の機器からデータ送信を要求され、その要求に対するアクセス権をアクセス可否判定部に問い合わせるときに、クライアント機器であることを証明するための第1の証明書と当該他の機器を証明するための第2の証明書とを付加してアクセス可否判定部に問い合わせ、アクセス可否判定部は、第1および第2の証明書を用いてアクセス可否問い合わせ部からの問い合わせを認証した後、アクセス権を判断し判断結果を返信する。

【0020】第7の発明によれば、サーバは、第1および第2の証明書を認証して、正しいクライアント機器か

【0021】第8の発明は、第7の発明に従属する発明であって、証明書にはX. 509を使用することを特徴とする。

【0022】第8の発明によれば、サーバは、X. 509方式の証明書を用いて、容易かつ確実に正しいクライアント機器からの通信であることを確認することができる。

【0023】第9の発明は、エンドユーザが所有する第1のクライアント機器に対して、第2のクライアント機器が直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を判断するためのアクセス権制御システムであって、少なくとも第2のクライアント機器と通信可能に接続され、少なくとも第1および第2のクライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するサーバを備え、サーバは、アクセス権の問い合わせに対してアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を返信するアクセス可否判定部を含み、第2のクライアント機器は、第1のクライアント機器に対して直接的なデータ送信を要求する際に、その要求に対するアクセス権をアクセス可否判定部に問い合わせるアクセス可否問い合わせ部と、アクセス可否問い合わせ部によって問い合わせた結果、アクセス可否判定部から返信された判断結果がアクセス可の場合、第1のクライアント機器に対して当該判断結果を附加して直接的なデータ送信を要求するデータ要求部とを含み、第1のクライアント機器は、データ要求部から送信された判断結果がアクセス可の場合、データ要求部から要求されたデータを第2のクライアント機器に対して直接的に送信するデータ送信部を含み、第2のクライアント機器は、さらにデータ要求部からの要求に応じてデータ送信部から送信されたデータを直接的に受信するデータ受信部とを含む。

【0024】第9の発明によれば、データの提供先となる第2のクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0025】第10の発明は、第9の発明に従属する発明であって、サーバが管理するアクセス権管理リストに

アクセス可能な機器を示すアクセス権が記述され、アクセス可否問い合わせ部は、データ送信を要求するデータ毎に、アクセス可否判定部に問い合わせを行い、アクセス可否判定部は、アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果を返信する。

【0026】第11の発明は、第10の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、アクセス可能な時間を示す時間条件がデータ毎に記述され、アクセス可否判定部は、アクセス可否問い合わせ部から問い合わせされた現在時刻に応じて時間条件を参照して、データ毎にそのアクセス権を判断する。

【0027】第12の発明は、第10の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、アクセス可能な回数を示す回数条件がデータ毎に記述され、アクセス可否判定部は、アクセス可否問い合わせ部から問い合わせされた回数に応じて回数条件を参照して、データ毎にそのアクセス権を判断する。

【0028】第13の発明は、第10の発明に従属する発明であって、さらに、サーバが管理するアクセス権管理リストには、データ毎に提供された当該データの複製に関する制限を示す複製条件が記述され、アクセス可否判定部は、アクセス可否問い合わせ部によるデータ毎の問い合わせに応じて、そのアクセス権を判断し判断結果と共に複製条件を返信し、データ要求部は、アクセス可否判定部から返信された判断結果がアクセス可の場合、第1のクライアント機器に対して判断結果および複製条件と共に直接的なデータ送信を要求し、データ送信部は、データ要求部から送信された判断結果がアクセス可の場合、データ要求部から要求されたデータと共に複製条件をデータ受信部に対して直接的に送信し、データ受信部は、データ送信部から送信されたデータを直接的に受信し、そのデータが複製条件によってその後の複製が制限される。

【0029】第13の発明によれば、データの提供先のクライアント機器からサーバにアクセス権を問い合わせする場合でも、それぞれのクライアント機器が管理するデータ毎に、データ取得後の複製に関する制限を付加することが可能となる。

【0030】第14の発明は、第9の発明に従属する発明であって、サーバは、他のプロキシを介して第2のクライアント機器と通信可能に接続されていることを特徴とする。

【0031】第14の発明によれば、アクセス権を問い合わせる提供先の第2のクライアント機器がサーバと直接通信が不可能であっても、他のプロキシを介してアクセス権の問い合わせが可能となり、ピアツーピアでのデータ交換が可能となる。

サーバ側で行うことができる。

【0032】第15の発明は、第9の発明に從属する発明であって、アクセス可否問い合わせ部は、第1のクライアント機器に対してデータ送信を要求するために、その要求に対するアクセス権をアクセス可否判定部に問い合わせるときに、第2のクライアント機器であることを証明するための証明書を附加してアクセス可否判定部に問い合わせ、アクセス可否判定部は、証明書を用いてアクセス可否問い合わせ部からの問い合わせを認証した後、アクセス権を判断し判断結果を返信する。

【0033】第15の発明によれば、サーバは、証明書を認証して、第2のクライアント機器からの通信であることを確認することができる。

【0034】第16の発明は、第15の発明に従属する発明であって、さらに、アクセス可否判定部は、判断結果にサーバの判断であることを証明するための署名を付加して返信し、データ要求部は、アクセス可否判定部から返信された判断結果がアクセス可の場合、第1のクライアント機器に対して署名が付加された判断結果および証明書と共に直接的なデータ送信を要求し、データ送信部は、データ要求部から送信された判断結果の署名を用いて認証を行い当該判断結果がアクセス可の場合、データ要求部から要求されたデータと共に複製条件をデータ受信部に対して直接的に送信する。

【0035】第16の発明によれば、この署名によって、アクセス権の判断結果の通信途上での改竄を防止することができ、第1のクライアント機器において、確実にサーバが判定した結果であることを判断することができる。

【0036】第17の発明は、第15の発明に従属する発明であって、証明書にはX. 509を使用することを特徴とする。

【0037】第18の発明は、エンドユーザが所有する複数のクライアント機器同士で当該クライアント機器が管理するデータを直接的に送受信を行う際に、そのアクセス可否を示すアクセス権を判断するサーバであって、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理部と、クライアント機器から送信されるアクセス権の問い合わせに対し、アクセス権管理部においてアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を問い合わせたクライアント機器に対して返信するアクセス可否判定部を含む。

【0038】第18の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバで行うことにより、データ交換を行うクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能なサーバを構成できる。

—タ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎にアクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるエンドユーザが所有するクライアント機器であって、他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をサーバに問い合わせるアクセス可否問い合わせ部と、アクセス可否問い合わせ部によって問い合わせた結果、サーバから返信された判断結果がアクセス可の場合、他の機器の要求に応じて直接的にデータ送信を行うデータ送信部とを含む。

【0040】第19の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバで行うことにより、データ送信を要求されたクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能なクライアント機器を構成できる。また、提供元のクライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0041】第20の発明は、他の機器に直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を、機器毎にアクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるエンタープライズユーザが所有するクライアント機器であって、他の機器に直接的なデータ送信を要求する際に、その要求に対するアクセス権をサーバに問い合わせるアクセス可否問い合わせ部と、アクセス可否問い合わせ部によって問い合わせた結果、サーバから返信された判断結果がアクセス可の場合、他の機器に対して当該判断結果を付加して直接的なデータ送信を要求するデータ要求部とを含む。

【0042】第20の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバで行うことにより、データ送信を要求するクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能なクライアント機器を構成できる。また、提供元および提供先のクライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0043】第21の発明は、他の機器から要求されることによって直接的なデータ送信を行うエンドユーザが所有するクライアント機器であって、他の機器からの直

れる当該データ送信に対するアクセス可否を示すアクセス権の判断結果とを受信する受信部と、受信部で受信した判断結果がアクセス可の場合、他の機器から要求されたデータを直接的に送信するデータ送信部を含む。

【0044】第21の発明によれば、ピアツーピアでのデータ交換を行う際のアクセス権の判断結果がデータ送信の要求と共に送信されることにより、データ送信を要求されたクライアント機器は、その判断結果に基づいてアクセス可否を判断可能であるため、複雑なアクセス権制御であっても適切に処理することが可能なクライアント機器を構成できる。また、提供元のクライアント機器が処理能力の限られた民生機器で構成されている場合でも、提供元のクライアント機器でアクセス権の制御が不要であるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、複雑なアクセス権制御を付加して容易に行うことが可能である。

【0045】第22の発明は、第21の発明に従属する発明であって、判断結果には、アクセス権の判断をした機器であることを証明するための署名が付加されており、データ送信部は、判断結果の署名に対する認証を行うことによって当該判断結果の正当性を評価し、当該判断結果が正当かつアクセス可の場合、他の機器から要求されたデータを直接的に送信する。

【0046】第22の発明によれば、データ送信の要求と共に送信されるピアツーピアでのデータ交換を行う際のアクセス権の判断結果を、署名によってアクセス権の判断結果の通信途上での改竄を防止することができ、提供元のクライアント機器において、確実に正当性を認証することができる。

【0047】第23の発明は、エンドユーザが所有するクライアント機器に対して他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断するためのアクセス権制御方法であって、サーバにおいて、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をクライアント機器からサーバに問い合わせるアクセス可否問い合わせステップと、アクセス可否問い合わせステップによる問い合わせに対して、アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権をサーバで判断し判断結果をクライアント機器に返信するアクセス可否判定ステップと、アクセス可否判定ステップによって返信された判断結果がアクセス可の場合、第1のクライアント機器に対して判断結果を付加して直接的なデータ送信を要求するデータ要求ステップと、データ要求ステップによって送信された判断結果がアクセス可の場合、データ要求ステップによって要求されたデータを第2のクライアント機器に対して直接的に送信するデータ送信ステップと、データ送信ステップによって第1のクライアント機器から送信されたデータを第2のクライアント機器で直接的に受信するデータ受信ステップとを含む。

【0048】第23の発明によれば、データの提供元と

とによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0049】第24の発明は、エンドユーザが所有する第1のクライアント機器に対して、第2のクライアント機器が直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を当該第2のクライアント機器と通信可能に接続されたサーバで判断するためのアクセス権制御方法であって、サーバにおいて、少なくとも第1および第2のクライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、第2のクライアント機器が第1のクライアント機器に直接的なデータ送信を要求する際に、その要求に対するアクセス権を第2のクライアント機器からサーバに問い合わせるアクセス可否問い合わせステップと、アクセス可否問い合わせステップによる問い合わせに対して、アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権をサーバで判断し判断結果を第2のクライアント機器に返信するアクセス可否判定ステップと、アクセス可否判定ステップから返信された判断結果がアクセス可の場合、第1のクライアント機器に対して判断結果を付加して直接的なデータ送信を要求するデータ要求ステップと、データ要求ステップによって送信された判断結果がアクセス可の場合、データ要求ステップによって要求されたデータを第2のクライアント機器に対して直接的に送信するデータ送信ステップと、データ送信ステップによって第1のクライアント機器から送信されたデータを第2のクライアント機器で直接的に受信するデータ受信ステップとを含む。

【0050】第24の発明によれば、データの提供元となる第2のクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。

器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0051】第25の発明は、エンドユーザが所有するクライアント機器同士で当該クライアント機器が管理するデータを直接的に送受信を行う際に、そのアクセス可否を示すアクセス権を当該クライアント機器と通信可能に接続されたサーバで判断させるためのアクセス権制御プログラムを記録した当該サーバが読み取り可能な記録媒体であって、クライアント機器のアクセス権を予め記述したアクセス権管理リストを管理するアクセス権管理ステップと、クライアント機器がデータの直接的な送受信を行なう際に、当該クライアント機器からサーバに対して行われるその送受信に対するアクセス権の問い合わせに応じて、アクセス権管理ステップで管理されているアクセス権管理リストを参照することによって、そのアクセス権を判断し判断結果を当該クライアント機器に返信するアクセス可否判定ステップとを含む。

【0052】第25の発明によれば、ピアツーピアでのデータ交換を行なう際のアクセス権の制御を処理能力の高いサーバで行なうことにより、データ交換を行なうクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能となる。

【0053】第26の発明は、他の機器から直接的なデータ送信を要求された際に、そのアクセス可否を示すアクセス権を、機器毎にアクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるアクセス権制御プログラムを記録したエンドユーザが所有するクライアント機器が読み取り可能な記録媒体であって、クライアント機器が他の機器から直接的なデータ送信を要求された際に、その要求に対するアクセス権をサーバに問い合わせるアクセス可否問い合わせステップと、アクセス可否問い合わせステップによって問い合わせた結果、サーバから返信された判断結果がアクセス可の場合、要求されたデータをクライアント機器から他の機器に対して直接的に送信するデータ送信ステップとを含む。

【0054】第26の発明によれば、ピアツーピアでのデータ交換を行なう際のアクセス権の制御を処理能力の高いサーバで行なうことにより、データ送信を要求されたクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能となる。また、提供元のクライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアで

加して容易に行なうことが可能である。

【0055】第27の発明は、他の機器に直接的なデータ送信を要求する際に、そのアクセス可否を示すアクセス権を、機器毎にアクセス権を予め記述したアクセス権管理リストを管理する通信可能なサーバに判断させるアクセス権制御プログラムを記録したエンドユーザが所有するクライアント機器が読み取り可能な記録媒体であって、他の機器に直接的なデータ送信を要求する際に、その要求に対するアクセス権をサーバに問い合わせるアクセス可否問い合わせステップと、アクセス可否問い合わせステップによって問い合わせた結果、サーバから返信された判断結果がアクセス可の場合、他の機器に対して当該判断結果を付加して直接的なデータ送信を要求するデータ要求ステップとを含む。

【0056】第27の発明によれば、ピアツーピアでのデータ交換を行なう際のアクセス権の制御を処理能力の高いサーバで行なうことにより、データ送信を要求するクライアント機器からアクセス権を問い合わせることによって、複雑なアクセス権制御であっても適切に処理することが可能となる。また、提供元および提供先のクライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行なうことが可能である。

【0057】

【発明の実施形態】（第1の実施形態）図1を参照して、本発明の第1の実施形態に係るアクセス権制御システムの全体の構成について説明する。図1において、当該アクセス権制御システムは、サーバ11、アクセス権管理データベース12、第1のクライアント機器13、データ記憶装置14、第2のクライアント機器15、およびデータ記憶装置16を備えている。第1および第2のクライアント機器13および15は、エンドユーザが所有するCPUを備えた機器であり、互いに直接的に通信するピアツーピアコンピューティングを形成し、ピアツーピア型のファイル交換システムを形成するものである。また、サーバ11は、上記ピアツーピア型のファイル交換システム内に配置されているクライアント機器と通信可能に接続されており、少なくとも第1のクライアント機器13は、サーバ11に対してアクセス可能に構成されている。データ記憶装置14および16は、それぞれ第1および第2のクライアント機器13および15によって管理されるファイル等を格納する記憶装置である。アクセス権管理データベース12は、サーバ11によって管理される後述するアクセス権管理リスト等を格納する記憶装置である。

【0058】なお、当該実施形態の説明では、説明を単純化するために第2のクライアント機器15が、第1の

格納された所望のファイルの提供を受けるためにアクセスする場合を想定し、第1のクライアント機器13がアクセス先（以下、提供元と記載する）のクライアント機器、第2のクライアント機器15がアクセス元（以下、提供先と記載する）のクライアント機器として説明を行う。また、当該アクセス権制御システムにおいては、2つ以上のクライアント機器を配置することが可能であるが、ここでは、上記ファイルのアクセスに関連するクライアント機器のみを説明する。

【0059】次に、図2を参照して、サーバ11の内部構成を説明する。なお、図2は、サーバ11の内部構成を示す機能ブロック図である。図2において、サーバ11は、アクセス可否判定部111、データベース制御部112、およびクライアント間通信部113を備えている。クライアント間通信部113は、TCP/IP等のプロトコルを使用し、第1のクライアント機器13とサーバ11との間の通信を行う。データベース制御部112は、アクセス権管理データベース12に格納されているデータを制御している。例えば、データベース制御部112は、アクセス可否判定部111からアクセス権管理データベース12に格納されているデータを要求された場合、その要求に応じてアクセス権管理データベース12のデータを検索したり、検索後のデータの更新を行ったりする。また、データベース制御部112は、クライアント間通信部113を介して指示されるクライアント機器からの要求に応じて、アクセス権管理データベース12のデータを追加したり削除したりする。アクセス可否判定部111は、後述する第1のクライアント機器13からクライアント間通信部113を介してアクセス権判定を求められた場合、その内容からアクセス権管理データベース12のアクセス権管理リストを参照し、そのアクセス権判定結果をクライアント間通信部113に返す。また、その判定によって、当該アクセス権管理リストの更新が必要な場合、その更新をデータベース制御部112に指示する。

【0060】次に、図3を参照して、第1のクライアント機器13の内部構成について説明する。なお、図3は、第1のクライアント機器13の内部構成を示す機能ブロック図である。図3において、第1のクライアント機器13は、サーバ間通信部131、アクセス可否問い合わせ部132、データ送信部133、クライアント間通信部134、および記憶装置制御部135を備えている。サーバ間通信部131は、TCP/IP等のプロトコルを使用し、第1のクライアント機器13とサーバ11との間の通信を行う。また、クライアント間通信部134は、TCP/IP等のプロトコルを使用し、第1のクライアント機器13と第2のクライアント機器15の間の通信を行う。データ送信部133は、クライアント間通信部134を介して第2のクライアント機器15か

れた場合、記憶装置制御部135を介して、データ記憶装置14に記憶されたデータの一覧を生成し、第2のクライアント機器15に当該データ一覧を提供する。また、データ送信部133は、サーバ11からアクセスが可能であることを通知された場合、記憶装置制御部135を介してデータ記憶装置14から要求のあったデータを取得し、このデータをクライアント間通信部134を制御して第2のクライアント機器15に送信する。アクセス可否問い合わせ部132は、第2のクライアント機器15からデータの要求を受け付けた場合、当該データの提供可否を判定するために、サーバ11へサーバ間通信部131を介して問い合わせを行う。また、第1のクライアント機器13は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第1のクライアント機器13に設けられたCPU固有の情報でもよいし、IPアドレスでもかまわない。

【0061】次に、図4を参照して、第2のクライアント機器15の内部構成について説明する。なお、図4は、第2のクライアント機器15の内部構成を示す機能ブロック図である。図4において、第2のクライアント機器15は、クライアント間通信部151、データ要求部152、データ受信部153、記憶装置制御部154、表示装置155、および入力装置156を備えている。クライアント間通信部151は、TCP/IP等のプロトコルを使用し、第1のクライアント機器13と第2のクライアント機器15の間の通信を行う。表示装置155は、例えば第1のクライアント機器13からクライアント間通信部151を介して受け取った上記データ一覧を表示することによって、第2のクライアント機器15の利用者にデータ一覧からの選択を促す。入力装置156は、利用者の操作によって所望のデータを上記データ一覧から選択する。データ要求部152は、利用者によって選択されたデータを取得すべく、第1のクライアント機器13にデータ要求のための通信をクライアント間通信部151を介して行う。データ受信部153は、上記データ要求が許可された場合、第1のクライアント機器13からクライアント間通信部151を介して当該データを受け取り、記憶装置制御部154がデータ記憶装置16を制御して当該データをデータ記憶装置16に格納する。また、第2のクライアント機器15は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第2のクライアント機器15に設けられたCPU固有の情報でもよいし、IPアドレスでもかまわない。

【0062】なお、当該実施形態では、第1および第2のクライアント機器13および15において、それぞれ内部構成が異なる場合を記述した。このような相違は、上述したように第1のクライアント機器13がデータの

提供先と想定していることに起因する。したがって、第1および第2のクライアント機器13および15が提供元にも提供先にもなり得る方が都合が良い場合には、それぞれのクライアント機器に両方のクライアント機器が備える機能を備えれば良い。

【0063】次に、図5を参照して、アクセス権制御システムの全体処理について説明する。なお、図5は、アクセス権制御システムを構成するサーバ11、第1および第2のクライアント機器13および15が処理する動作を示すフローチャートである。ここで説明するアクセス権制御システムの全体処理についても、第1のクライアント機器13がデータの提供元であり、第2のクライアント機器15がデータの提供先と想定し、第2のクライアント機器15が第1のクライアント機器13に管理されているデータ記憶装置14に格納された所望のデータを取得する場合について説明する。なお、このアクセス権制御システムの処理動作は、サーバ11、第1および第2のクライアント機器13および15において、各機器に対応するアクセス権制御プログラムが各機器に備えられている記憶領域に格納され実行されることによって行われる。しかしながら、これらのアクセス権制御プログラムは、サーバ11、第1および第2のクライアント機器13および15が、各機器に対応するそれらを読み出して実行可能である限りにおいて、各機器に備えられている記憶領域以外の他の記憶媒体に格納されていてもかまわない。

【0064】図5において、第2のクライアント機器15のデータ要求部152は、第1のクライアント機器13が管理するデータの一覧を要求するために、その内容が記述されたデータ一覧を第1のクライアント機器13に要求する（ステップS1）。ステップS1では、第2のクライアント機器15の利用者が入力装置156を操作することによって、データ要求部152にデータ一覧の要求が伝達される。そして、データ要求部152によって、クライアント間通信部151を介して、第1のクライアント機器13に上記データ一覧が要求される。

【0065】次に、第1のクライアント機器13のクライアント間通信部134は、第2のクライアント機器15からデータ一覧が要求され、当該データ一覧の要求をデータ送信部133に伝える（ステップS2）。次に、データ送信部133は、記憶装置制御部135を制御することによってデータ記憶装置14で管理されているデータを検索し、データ記憶装置14で管理されているデータ一覧を作成する（ステップS3）。そして、データ送信部133は、上記ステップS3で作成したデータ一覧を、クライアント間通信部134を介して第2のクライアント機器15に送信する（ステップS4）。

【0066】次に、第2のクライアント機器15のクライアント間通信部151は、上記ステップS4で第1の

し、第2のクライアント機器15の表示装置155によって受信したデータ一覧が表示される（ステップS5）。次に、第2のクライアント機器15の利用者は、表示装置155に表示されたデータ一覧から所望のデータを選択し、入力装置156を操作することによって選択結果をデータ要求部152に伝達する（ステップS6）。そして、データ要求部152は、ステップS6で選択されたデータを識別する提供対象ファイル名および自身を判別するための提供先識別子（つまり、第2のクライアント機器15の識別子）を、クライアント間通信部151を介して送信することによって、第1のクライアント機器13にデータを要求する（ステップS7）。

【0067】次に、第1のクライアント機器13のクライアント間通信部134は、第2のクライアント機器15から要求された上記提供対象ファイル名および上記提供先識別子を受信し、当該要求をアクセス可否問い合わせ部132に送る（ステップS8）。次に、アクセス可否問い合わせ部132は、第2のクライアント機器15から要求されたデータに対するアクセスの可否を判定するために、当該要求に対するアクセス権問い合わせとして、上記提供対象ファイル名、上記提供先識別子、および自身を判別するための提供元識別子（つまり、第1のクライアント機器13の識別子）を、サーバ間通信部131を介してサーバ11に送信する（ステップS9）。

【0068】次に、サーバ11のクライアント間通信部113は、第1のクライアント機器13からアクセス権問い合わせとして送信された、上記提供対象ファイル名、上記提供先識別子、および上記提供元識別子を、アクセス可否判定部111に送る（ステップS10）。次に、アクセス可否判定部111は、上記アクセス権問い合わせに対して、データベース制御部112を制御してアクセス権管理データベース12に格納されているアクセス権管理リストを参照して、要求されているデータのアクセス権を判定する（ステップS11）。なお、ステップS11におけるアクセス権判定処理についての詳細な動作は、後述する。そして、アクセス可否判定部111は、ステップS11で要求されたデータに対するアクセス権を判定した結果を、クライアント間通信部133を介して第1のクライアント機器13に送信する（ステップS12）。また、上記ステップS11でアクセス権管理リストから参照した登録データにおいて、後述する「複製条件」の制限が記述されている場合、上記ステップS12での複製条件を示す情報（以下、複製条件情報と記載する）も同時に第1のクライアント機器13に送信される。

【0069】次に、第1のクライアント機器13のサーバ間通信部131は、サーバ11から送信されたアクセス権判定結果を受信し、データ送信部133に送る（ステップS13）。次に、データ送信部133は、上記ス

たデータのアクセス可否を上記アクセス権判定結果から判断する（ステップS14）。データ送信部133は、上記アクセス権判定結果がアクセス可であった場合、上記ステップS8で第2のクライアント機器15から要求されたデータを、記憶装置制御部135を制御することによってデータ記憶装置14から検索し、当該データをクライアント間通信部134を介して第2のクライアント機器15に送信する（ステップS15）。また、上記ステップS12で複製条件情報も同時に送信されている場合、要求されたデータは、その複製条件情報と共に第2のクライアント機器15に送信される。一方、上記アクセス権判定結果がアクセス不可であった場合、第2のクライアント機器15に対するデータ送信を拒否する。

【0070】次に、第2のクライアント機器15のクライアント間通信部151は、上記ステップS15で送信されたデータを受信し、データ受信部153に送る（ステップS16）。そして、データ受信部153は、記憶装置制御部154を制御することによって、上記ステップS16で受信したデータをデータ記憶装置16に格納したり、表示装置155に当該データを表示したりする。また、上記ステップS16で受信したデータが上記複製条件情報と共に受信された場合、当該データは以後の複製に関して、当該複製条件情報に制限される。なお、この複製の制限については、後述する。

【0071】次に、図6を参照して、アクセス権管理データベース12に格納されているアクセス権管理リストのデータ構造について説明する。なお、図6は、アクセス権管理データベース12に格納されているアクセス権管理リストの一例である。図6において、アクセス権管理データベース12に格納されているアクセス権管理リストに登録されるデータは、「番号」、「提供元識別子」、「ファイル名」、「提供先識別子」、「時間条件」、「回数条件」、および「複製条件」の7つの項目から構成されている。

【0072】上記アクセス権管理リストの「番号」は、アクセス権管理データベース12において、各登録データを管理するために使用する重複を避けた自然数の番号である。

【0073】上記アクセス権管理リストの「提供元識別子」は、データの提供元である端末（つまり、提供元のクライアント機器）を特定するため、各クライアント機器固有の識別子である。

【0074】上記アクセス権管理リストの「ファイル名」は、アクセス対象となるデータのファイル名である。なお、このファイル名は、コンテンツに固有の識別情報であるコンテンツIDを記載してもかまわない。

【0075】上記アクセス権管理リストの「提供先識別子」は、データの提供先である端末（つまり、提供先のクライアント機器）を特定するため、各クライアント

には、特定のクライアント機器が指定されるのみではなく、任意のクライアント機器に対してアクセスが許可される場合、「任意」と記述される。また、全てのクライアント機器に対してアクセスの許可をしない場合、「不可」と記述あるいは未記述とされる。

【0076】上記アクセス権管理リストの「時間条件」は、データの提供が許可される期日を指定したり、データの提供が許可される期間を指定したりするアクセス許可を行う時間的な制限である。なお、そのデータのアクセスに時間的な制限を設けない場合、「任意」と記述される。

【0077】上記アクセス権管理リストの「回数条件」は、データの提供元である端末から、データの提供が許可される回数に関する条件である。この「回数条件」に、上記回数が設定されるデータでは、サーバ11がそのデータに対するアクセス権を付与すると「回数条件」が更新され、「回数条件」が「0回」に更新された時点で、以降のアクセスが許可されなくなる。なお、アクセス権管理リストのデータに回数に関する条件を設けない場合、「任意」と記述される。

【0078】上記アクセス権管理リストの「複製条件」は、提供されたデータを提供先の端末において更に複製することが許可されるか否かを示す条件である。この「複製条件」には、登録データに対して提供後の複製が許可されていない場合、「不可」と記述され、特に複製に関する条件を設けない場合、「任意」と記述され、複製世代数を制限する場合、その世代数（例えば、「番号」「4」に記述された「1世代のみ可」）が記述される。

【0079】上述した項目毎に、登録データがアクセス権管理リストに記述される。例えば、「番号」が「1」の登録データは、「提供元識別子」が「1111」に端末に記憶されている「ファイル名」「産声.wav」という音声ファイルに関するアクセス権を管理するための登録データである。この音声ファイルには、「提供先識別子」が「2222」の端末のみがアクセスすることが可能である。そして、上記「2222」の端末がアクセスの日時や回数に関する制約は設けられていない。ただし、提供先の「2222」の端末では、提供されたファイル「産声.wav」を更に複製することは禁止されている。

【0080】また、例えば、「番号」が「4」の登録データは、「提供元識別子」が「1111」の端末に記憶されている「ファイル名」「子供.jpg」という画像ファイルに関するアクセス権を管理するための登録データである。この画像ファイルには、「提供先識別子」が「2222」および「3333」の端末のみがアクセスすることが可能である。そして、上記「2222」および「3333」の端末がアクセス可能な日時は、「2011/11/11 11:11:11」～「2011/11/11 11:11:11」

月31日までアクセス可能であり、それ以降はアクセス不可能である。なお、上記「2222」および「3333」の端末がアクセスする回数に関する制約はない。また、提供先の「2222」および「3333」端末では、提供されたファイル「子供.jpg」を更に1世代のみ複製することが許可されている。

【0081】さらに、「番号」が「9」の登録データは、特殊なアクセス権を管理するための登録データである。この登録データでは、「提供元識別子」が「4444」の端末が、「提供先識別子」が「1111」の端末に対するアクセス権管理用のデータであるが、「ファイル名」に関しては「任意」となっている。つまり、当該「4444」の端末に格納された全てのファイルに対して、「1111」の端末がアクセス可能ということを意味している。このような利用形態は、「番号」が「1111」および「4444」の端末の所有者が同一人物であり、相互にファイルアクセスを無条件に許可する場合などに利用される。

【0082】なお、上述したアクセス権管理データベース12に格納されているアクセス権管理リストに記述される登録データは、以下の条件によって記述することができる。

条件1：サーバ11がアクセス権を管理する全てのクライアント機器が管理しているデータの内、他のクライアント機器に提供可能あるいは何らかの条件を付与して提供可能なデータを、アクセス権管理リストに記述する。

（つまり、アクセス権管理リストに記述されていないデータはアクセス不可）

条件2：サーバ11がアクセス権を管理する全てのクライアント機器が管理しているデータの内、他のクライアント機器に提供不可能あるいは何らかの条件を付与して提供可能なデータを、アクセス権管理リストに記述する。（つまり、アクセス権管理リストに記述されていないデータはアクセス可）

【0083】次に、上記ステップS11（図5を参照）でアクセス可否判定部111が行うアクセス権判定処理について、詳細な動作を説明する。なお、図7は、アクセス可否判定部111が行うアクセス権判定処理の詳細動作の一例を示す上記ステップS11のサブルーチンである。また、上述したアクセス権管理データベース12に格納されているアクセス権管理リストに記述される登録データは、上記条件1（つまり、アクセス権管理リストに記述されていないデータは、アクセス不可）に基づいて記述されているとして説明を行う。

【0084】図7において、アクセス可否判定部111は、提供元のクライアント機器を判別するための提供元識別子、提供先のクライアント機器を判別するための提供先識別子、および提供対象となるデータを識別するための提供対象ファイル名が記述されたアクセス権問い合わせ

可否判定部111は、当該サブルーチンで利用する一時変数であるnを初期化するために、1にセットする（ステップS112）。

【0085】次に、アクセス可否判定部111は、上記ステップS111で取得した提供元識別子と、アクセス権管理データベース12に格納されている上記アクセス権管理リストに記述されている「番号」が「n」の登録データの「提供元識別子」とが一致しているか否かを判定する（ステップS113）。そして、アクセス可否判定部111は、上記ステップS113で一致している場合、次のステップS114に処理を進める。一方、アクセス可否判定部111は、上記ステップS113で一致していない場合、次のステップS119に処理を進める。

【0086】ステップS114では、アクセス可否判定部111は、上記ステップS111で取得した提供対象ファイル名と、上記アクセス権管理リストに記述されている「番号」が「n」の登録データの「ファイル名」とが一致しているか否かを判定する。なお、上述したようにアクセス権管理リストの「ファイル名」には、「任意」と設定されていることもある。この場合、アクセス可否判定部111は、上記ステップS111で取得した提供対象ファイル名が、アクセス権管理リストの「ファイル名」と一致していると判断する。そして、アクセス可否判定部111は、上記ステップS114で一致している場合、次のステップS115に処理を進める。一方、アクセス可否判定部111は、上記ステップS114で一致していない場合、次のステップS119に処理を進める。

【0087】ステップS115では、アクセス可否判定部111は、上記ステップS111で取得した提供先識別子と、上記アクセス権管理リストに記述されている「番号」が「n」の登録データの「提供先識別子」とが一致しているか否かを判定する。なお、上述したようにアクセス権管理リストの「提供先識別子」には、「任意」と設定されていることもある。この場合、アクセス可否判定部111は、上記ステップS111で取得した提供先識別子が、アクセス権管理リストの「提供先識別子」と一致していると判断する。そして、アクセス可否判定部111は、上記ステップS115で一致している場合、次のステップS116に処理を進める。一方、アクセス可否判定部111は、上記ステップS115で一致していない場合、次のステップS119に処理を進める。

【0088】ステップS116では、アクセス可否判定部111は、現在時刻と上記アクセス権管理リストに記述されている「番号」が「n」の登録データの「時間条件」とを比較し、アクセス可否を判定する。このアクセス可否判定部111が行う上記比較は、「時間条件」に

れ、「時間条件」に時間的な制約が記述されている場合、現在時刻がその制約を満足するか否かで判定される。そして、アクセス可否判定部111は、上記ステップS116でアクセス可と判断した場合、次のステップS117に処理を進める。一方、アクセス可否判定部111は、上記ステップS116でアクセス不可と判断した場合、次のステップS119に処理を進める。

【0089】ステップS117では、アクセス可否判定部111は、上記アクセス権管理リストに記述されている「番号」が「n」の登録データの「回数条件」を参照してアクセス可否を判定する。このアクセス可否判定部111が行う上記判定は、「回数条件」に「任意」あるいは「1回以上の回数」が記述されている場合、アクセス可と判定され、「回数条件」に「0回」が記述されている場合、アクセス不可と判定される。また、アクセス可否判定部111は、「回数条件」に「1回以上の回数」が記述され、アクセス可と判定した後、当該「回数条件」に記述されている回数を1だけ減らしてアクセス権管理リストを更新する。そして、アクセス可否判定部111は、上記ステップS117でアクセス可と判定した場合、次のステップS118に処理を進める。一方、アクセス可否判定部111は、上記ステップS117でアクセス不可と判断した場合、次のステップS119に処理を進める。

【0090】なお、上記ステップS117では、上記アクセス権管理リストの「回数条件」の更新として、アクセス可と判定された場合にどのクライアント機器からのアクセスにおいても必ず回数を1回減らす方法を説明した。しかしながら、複数の「提供先識別子」が設定されている場合、それらのクライアント機器が1つの「回数条件」を共有するのではなく、データの提供先の各クライアント機器毎に「回数条件」を持たせてもかまわない。

【0091】ステップS118では、アクセス可否判定部111は、上記ステップS111で取得したアクセス権問い合わせに対して、アクセス可と判断し、当該サブルーチンを終了する。なお、このステップS118の処理には、上述したステップS113～S117でアクセス可否判定部111が上記ステップS111で取得したアクセス権問い合わせの内容に一致し、かつアクセス条件を全て満たす場合のみ進むことができるため、アクセス可否判定部111は、上記アクセス権管理リストの登録データ記述に一致し、それぞれの条件を満たすクライアント機器にのみアクセス可の判定を行うことになる。

【0092】一方、上述したように、アクセス可否判定部111は、上記ステップS111で取得したアクセス権問い合わせが、上記ステップS113～S117で判定したいずれかの結果を満たさない場合、ステップS119に処理を進める。ステップS119では、アクセス

変数であるnを1だけ増やしてn+1として、ステップS120に処理を進める。

【0093】ステップS120では、アクセス可否判定部111は、現在の一時変数であるnが上記アクセス権管理リストのデータ登録数であるNより大きいか否かを判断する。そして、アクセス可否判定部111は、n>Nの場合、上記アクセス権管理リストの登録データを全て探索したと判断して、次のステップS121に処理を進める。一方、アクセス可否判定部111は、n≤Nの場合、上記アクセス権管理リストに探索されていない登録データがあると判断して、上記ステップS113に戻り、上記ステップS119で設定した新たな「番号」に対して同様の探索を行う。

【0094】ステップS121では、アクセス可否判定部111は、上記ステップS111で取得したアクセス権問い合わせに対して、アクセス不可と判断し、当該サブルーチンを終了する。なお、このステップS121の処理には、上述したステップS113～S117でアクセス可否判定部111が上記ステップS111で取得したアクセス権問い合わせの内容が一致しない、あるいはアクセス条件のいずれかが満たさない場合に処理される。つまり、アクセス可否判定部111は、アクセス権問い合わせの内容が、上記アクセス権管理リストの登録データ記述のいずれかに一致しない、あるいは、それぞれの条件のいずれかを満たさないクライアント機器に対しては、アクセス不可の判定を行うことになる。

【0095】なお、上述した図7で示したアクセス可否判定部111が行うアクセス権判定処理は、アクセス権管理データベース12に格納されているアクセス権管理リストに記述される登録データが、上記条件1に基づいて記述されているとして説明したが、上記登録データが、上記条件2（つまり、アクセス権管理リストに記述されていないデータはアクセス可）に基づいて記述されてもかまわない。その場合、上述した図7で示したアクセス可否判定部111が行うアクセス権判定処理の動作手順を、以下に述べるステップのみ変更することによって対応可能である。つまり、図8を参照して、アクセス可否判定部111は、上記ステップS115～S117で「n○」と判定した場合、上記ステップS121に処理を進め、上記ステップS111で取得したアクセス権問い合わせに対して、アクセス不可と判断し、当該サブルーチンを終了する。また、アクセス可否判定部111は、上記ステップS120でn>Nの場合、上記ステップS118に処理を進め、上記ステップS111で取得したアクセス権問い合わせに対して、アクセス可と判断し、当該サブルーチンを終了する。このように、アクセス可否判定部111は、複数の記述条件で記述されたアクセス権管理リストに対して、その記述条件に応じた動作手順を用いることによって、適切にアクセス可否

【0096】なお、第1の実施形態の説明では、第1および第2のクライアント機器13および15の認証に関する手法を記述していないが、サーバ11と第1および第2のクライアント機器13および15との間で、認証によって正しいクライアント機器からの通信であることを確認してもかまわない。つまり、第2のクライアント機器15から第1のクライアント機器13への通信の際には、第2のクライアント機器15であることを証明するための第2のクライアント証明書を送信し、第1のクライアント機器13からサーバ11への通信の際には、上記第2のクライアント証明書および第1のクライアント機器13であることを証明する第1のクライアント証明書を、サーバ11に送信することによって、サーバ11は、これらの証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。このときに用いられる証明書としては、例えば、電子鍵証明書および証明書失効リストの標準仕様であるX.509等を用いることができる。

【0097】また、サーバ11から第1のクライアント機器13に対して、アクセス権の判定結果と共に複製条件情報が送信される場合、サーバ11は、この複製条件情報に対して所定の暗号化を行う。例えば、サーバ11が所有する秘密鍵で上記複製条件情報に署名して送信することによって、この複製条件が適用されるデータが提供される第2のクライアント機器15に対して正当性が保証される。また、この複製条件が適用されるデータは、DRM(Digital Rights Management)方式で暗号化される。例えば、データの提供元である第1のクライアント機器13では、サーバ11からアクセス権の判定結果と共に複製条件情報が送信された場合、その複製条件情報が適用されるデータに対して第2のクライアント機器15が公開する公開鍵で暗号化し、上記複製条件情報と共に第2のクライアント機器15に送信する。そして、第2のクライアント機器15では、秘密鍵を耐タンパ領域に格納し、当該機器の利用者に対しても秘密になるように保持しておく。これによって、第2のクライアント機器15以外に上記データを不正にコピーした場合でもデータの復号化は不可能であり、実質的に複製が制限される。また、上記複製条件にしたがってコピーを行う場合には、暗号化されたデータを第2のクライアント機器15の秘密鍵で一度復号化し、再度複製先機器が公開する公開鍵を用いて暗号化することによって、複製を制限することが可能である。なお、ここではデータを直接公開鍵で暗号化するとしたが、データを共通鍵方式の暗号鍵で暗号化し、さらにここで使用した暗号鍵を第2のクライアント機器15が公開する公開鍵を用いて第1のクライアント機器13が暗号化し、暗号化したデータと共に暗号鍵を送信してもかまわない。なお、上記複製条件情報の署名が改竄されて

その複製条件情報が適用されるデータに対する複製は不可とされる。

【0098】また、サーバ11と第1および第2のクライアント機器13および15との間で行われる通信の経路に関する秘匿性・耐改竄性については、第1の実施形態では特に手法を記述していないが、秘密鍵方式とセッション鍵とを組み合わせた暗号化方式による暗号化通信を行ってもかまわない。このような暗号化通信としては、SSL(Secure Socket Layer)等を用いることができる。

【0099】また、第1の実施形態では、第1のクライアント機器13は、上記ステップS3において、自身が管理しているデータ記憶装置14に格納されたデータをデータ一覧として作成したが、第2のクライアント機器15がアクセス可能なデータのみを上記データ一覧として作成してもかまわない。これは、第1のクライアント機器13が、上記ステップS2で第2のクライアント機器15からデータ一覧要求を受信することによって、サーバ11に対して第2のクライアント機器15がアクセス可能なデータ返信するように、アクセス権問い合わせを行う。そのアクセス権問い合わせの結果、送信される第2のクライアント機器15に提供可能と判断されたデータに基づいて、上記データ一覧を作成することによって、アクセス可能なデータのみを上記データ一覧として作成することができる。なお、上記アクセス可能なデータのみが記載されたデータ一覧を用いて、第2のクライアント機器15がデータの要求を行った後も、第1のクライアント機器13は、再度サーバ11に対してアクセス権問い合わせを行ってもかまわない。

【0100】このように、第1の実施形態に係るアクセス権制御システムによれば、データの提供元となるクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0101】(第2の実施形態) 図9を参照して、本発明の第2の実施形態に係るアクセス権制御システムの全体の構成について説明する。なお、上述した第1の実施形態では、データの提供元であるクライアント機器(つづり)から受け取った複数のデータを、各機器が持つ

クセス権の問い合わせをサーバ11に対して行ったが、第2の実施形態では、データの提供先であるクライアント機器（つまり、アクセス元のクライアント機器）がアクセス権の問い合わせをサーバに対して行うアクセス権制御システムである。

【0102】図9において、当該アクセス権制御システムは、サーバ21、アクセス権管理データベース22、第1のクライアント機器23、データ記憶装置24、第2のクライアント機器25、およびデータ記憶装置26を備えている。第1および第2のクライアント機器23および25は、エンドユーザが所有するCPUを備えた機器であり、互いに直接的に通信するピアツーピアコンピューティングを形成し、ピアツーピア型のファイル交換システムを形成するものである。また、サーバ21は、上記ピアツーピア型のファイル交換システム内に配置されているクライアント機器と通信可能に接続されており、少なくとも第2のクライアント機器25は、サーバ21に対してアクセス可能に構成されている。データ記憶装置24および26は、それぞれ第1および第2のクライアント機器23および25によって管理されるファイル等を格納する記憶装置である。アクセス権管理データベース22は、サーバ21によって管理される後述するアクセス権管理リスト等を格納する記憶装置である。

【0103】なお、当該実施形態の説明では、説明を単純化するために第2のクライアント機器25が、第1のクライアント機器23が管理するデータ記憶装置24に格納された所望のファイルの提供を受けるためにアクセスする場合を想定し、第1のクライアント機器23がアクセス先（以下、提供元と記載する）のクライアント機器、第2のクライアント機器25がアクセス元（以下、提供先と記載する）のクライアント機器として説明を行う。また、当該アクセス権制御システムにおいては、2つ以上のクライアント機器を配置することが可能であるが、ここでは、上記ファイルのアクセスに関連するクライアント機器のみを説明する。

【0104】次に、図10を参照して、サーバ21の内部構成を説明する。なお、図10は、サーバ21の内部構成を示す機能ブロック図である。図10において、サーバ21は、アクセス可否判定部211、データベース制御部212、およびクライアント間通信部213を備えている。クライアント間通信部213は、TCP/IP等のプロトコルを使用し、第2のクライアント機器25とサーバ21との間の通信を行う。データベース制御部212は、アクセス権管理データベース22に格納されているデータを制御している。例えば、データベース制御部212は、アクセス可否判定部211からアクセス権管理データベース22に格納されているデータを要求された場合、その要求に応じてアクセス権管理データ

新を行ったりする。また、データベース制御部212は、クライアント間通信部213を介して指示されるクライアント機器からの要求に応じて、アクセス権管理データベース22のデータを追加したり削除したりする。アクセス可否判定部211は、後述する第2のクライアント機器25からクライアント間通信部213を介してアクセス権判定を求められた場合、その内容からアクセス権管理データベース22のアクセス権管理リストを参照し、そのアクセス権判定結果をクライアント間通信部213に返す。また、その判定によって、当該アクセス権管理リストの更新が必要な場合、その更新をデータベース制御部212に指示する。

【0105】次に、図11を参照して、第1のクライアント機器23の内部構成について説明する。なお、図11は、第1のクライアント機器23の内部構成を示す機能ブロック図である。図11において、第1のクライアント機器23は、クライアント間通信部231、データ送信部232、および記憶装置制御部233を備えている。クライアント間通信部231は、TCP/IP等のプロトコルを使用し、第1のクライアント機器23と第2のクライアント機器25の間の通信を行う。データ送信部232は、クライアント間通信部231を介して第2のクライアント機器25からデータ記憶装置24に格納されたデータの一覧を要求された場合、記憶装置制御部233を介して、データ記憶装置24に記憶されたデータの一覧を生成し、第2のクライアント機器25に当該データ一覧を提供する。また、データ送信部232は、第2のクライアント機器25からサーバ21がアクセスが可能であることを判定した結果が送信された場合、記憶装置制御部233を介してデータ記憶装置24から要求のあったデータを取得し、このデータをクライアント間通信部231を制御して第2のクライアント機器25に送信する。また、第1のクライアント機器23は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第1のクライアント機器23に設けられたCPU固有の情報でもよいし、IPアドレスでもかまわない。

【0106】次に、図12を参照して、第2のクライアント機器25の内部構成について説明する。なお、図12は、第2のクライアント機器25の内部構成を示す機能ブロック図である。図12において、第2のクライアント機器25は、サーバ間通信部251、アクセス可否問い合わせ部252、データ要求部253、クライアント間通信部254、記憶装置制御部255、およびデータ受信部256、表示装置257および入力装置258を備えている。サーバ間通信部251は、TCP/IP等のプロトコルを使用し、第2のクライアント機器25とサーバ21との間の通信を行う。また、クライアント間通信部254は、TCP/IP等のプロトコルを使用

機器 2 5 の間の通信を行う。表示装置 2 5 7 は、例えば第 1 のクライアント機器 2 3 からクライアント間通信部 2 5 4 を介して受け取った上記データ一覧を表示することによって、第 2 のクライアント機器 2 5 の利用者にデータ一覧からの選択を促す。入力装置 2 5 8 は、利用者の操作によって所望のデータを上記データ一覧から選択する。データ要求部 2 5 3 は、アクセス可否問い合わせ部 2 5 2 に利用者によって選択されたデータに対するアクセス権の判定の問い合わせを指示し、その判定結果に基づいて上記選択されたデータを取得すべく、第 1 のクライアント機器 2 3 にデータ要求のための通信をクライアント間通信部 2 5 4 を介して行う。アクセス可否問い合わせ部 2 5 2 は、データ要求部 2 5 3 からデータの要求を受け付けた場合、当該データのアクセス可否を判定するために、サーバ 2 1 へサーバ間通信部 2 5 1 を介して問い合わせを行う。データ受信部 2 5 6 は、上記アクセスが許可された場合、第 1 のクライアント機器 2 3 からクライアント間通信部 2 5 4 を介して当該データを受け取り、記憶装置制御部 2 5 5 がデータ記憶装置 2 6 を制御して当該データをデータ記憶装置 2 6 に格納する。また、第 2 のクライアント機器 2 5 は、固有の識別子を有しており、この識別子を識別子格納部（図示しない）に格納している。なお、上記識別子は、第 2 のクライアント機器 2 5 に設けられた C P U 固有の情報でもよいし、 I P アドレスでもかまわない。

【0107】なお、当該実施形態では、第1および第2のクライアント機器23および25において、それぞれ内部構成が異なる場合を記述した。このような相違は、上述したように第1のクライアント機器23がデータの提供元であり、第2のクライアント機器25がデータの提供先と想定していることに起因する。したがって、第1および第2のクライアント機器23および25が提供元にも提供先にもなり得る方が都合が良い場合には、それぞれのクライアント機器に両方のクライアント機器が備える機能を備えれば良い。

【0108】 次に、図13を参照して、第2の実施形態に係るアクセス権制御システムの全体処理について説明する。なお、図13は、アクセス権制御システムを構成するサーバ21、第1および第2のクライアント機器23および25が処理する動作を示すフローチャートである。ここで説明するアクセス権制御システムの全体処理についても、第1のクライアント機器23がデータの提供元であり、第2のクライアント機器25がデータの提供先と想定し、第2のクライアント機器25が第1のクライアント機器26に管理されているデータ記憶装置24に格納された所望のデータを取得する場合について説明する。なお、このアクセス権制御システムの処理動作は、サーバ21、第1および第2のクライアント機器23および25において、各機器に対応するアクセス権制御モジュールが各機器に備えられて、各機器が各モジュールによって操作される。

され実行されることによって行われる。しかしながら、これらのアクセス権制御プログラムは、サーバ21、第1および第2のクライアント機器23および25が、各機器に対応するそれらを読み出して実行可能である限りにおいて、各機器に備えられている記憶領域以外の他の記憶媒体に格納されていてもかまわない。

【0109】図13において、第2のクライアント機器25のデータ要求部253は、第1のクライアント機器23が管理するデータの一覧を要求するために、その内容が記述されたデータ一覧を第1のクライアント機器23に要求する（ステップS21）。ステップS21では、第2のクライアント機器25の利用者が入力装置258を操作することによって、データ要求部253にデータ一覧の要求が伝達される。そして、データ要求部253によって、クライアント間通信部254を介して、第1のクライアント機器23に上記データ一覧が要求される。

【0110】 次に、第1のクライアント機器23のクライアント間通信部231は、第2のクライアント機器25からデータ一覧が要求され、当該データ一覧の要求をデータ送信部232に伝える（ステップS22）。次に、データ送信部232は、記憶装置制御部233を制御することによってデータ記憶装置24で管理されているデータを検索し、データ記憶装置24で管理されているデータ一覧を作成する（ステップS23）。そして、データ送信部232は、上記ステップS23で作成したデータ一覧を、クライアント間通信部231を介して第2のクライアント機器25に送信する（ステップS24）。

【0111】 次に、第2のクライアント機器25のクライアント間通信部254は、上記ステップS24で第1のクライアント機器23から送信されたデータ一覧を受信し、第2のクライアント機器25の表示装置257によって受信したデータ一覧が表示される（ステップS25）。次に、第2のクライアント機器25の利用者は、表示装置257に表示されたデータ一覧から所望のデータを選択し、入力装置258を操作することによって選択結果をデータ要求部253に伝達する（ステップS26）。そして、データ要求部253は、ステップS26で選択されたデータを識別する提供対象ファイル名および提供元の端末を判別するための提供元識別子（つまり、第1のクライアント機器23の識別子）を、アクセス可否問い合わせ部252に送る。次に、アクセス可否問い合わせ部252は、データ要求部253によって要求されたデータに対するアクセスの可否を判定するために、当該要求に対するアクセス権問い合わせとして、上記提供対象ファイル名、上記提供元識別子、および自身を判別するための提供先識別子（つまり、第2のクライアント機器25の識別子）を、サーバ間通信部251を介してサードパーティに送信する（ここで、サードパーティ）。

【0112】次に、サーバ21のクライアント間通信部213は、第2のクライアント機器25からアクセス権問い合わせとして送信された、上記提供対象ファイル名、上記提供先識別子、および上記提供元識別子を、アクセス可否判定部211に送る（ステップS28）。次に、アクセス可否判定部211は、上記アクセス権問い合わせに対して、データベース制御部212を制御してアクセス権管理データベース22に格納されているアクセス権管理リストを参照して、要求されているデータのアクセス権を判定する（ステップS29）。なお、ステップS29におけるアクセス権判定処理については、後述する。そして、アクセス可否判定部211は、ステップS29で要求されたデータに対するアクセス権を判定した結果に対して所定の暗号化を行った後、クライアント間通信部213を介して第2のクライアント機器25に送信する（ステップS30）。また、上記ステップS29でアクセス権管理リストから参照した登録データにおいて、「複製条件」の制限が記述されている場合、上記ステップS30でその複製条件情報も同時に第2のクライアント機器25に送信される。

【0113】なお、上記ステップS30で行うアクセス権を判定した結果に対する暗号化は、サーバ21でのアクセス権の判定結果に対する正当性を保証するためである。例えば、上記アクセス権の判定結果を第1のクライアント機器23が公開する公開鍵で暗号化する、あるいは、サーバ21が所有する秘密鍵で署名したデータを付加して送信することによって、上記正当性が保証される。つまり、この暗号化によって、通信途上での改竄を防止することができ、後述する第1のクライアント機器23の正当性評価では、確実にサーバ21が判定した結果であることを判断することが可能である。

【0114】次に、第2のクライアント機器25のサーバ間通信部251は、サーバ21から送信されたアクセス権判定結果を受信し、データ要求部253に送る（ステップS31）。次に、データ要求部253は、上記アクセス権判定結果によって上記ステップS26で選択したデータに対するアクセスが可能か否かを判断する（ステップS32）。データ要求部253は、上記アクセス権判定結果がアクセス可であった場合、上記提供対象ファイル名をサーバ21から送信された上記アクセス権判定結果と共に、クライアント間通信部254を介して送信することによって、第1のクライアント機器23にデータを要求する（ステップS33）。また、上記ステップS30で複製条件情報も同時に送信されている場合、その複製条件情報と共に第1のクライアント機器23に要求される。一方、上記アクセス権判定結果がアクセス不可であった場合、第2のクライアント機器25は、第1のクライアント機器23に対するデータ要求を中止する。

クライアント間通信部231は、第2のクライアント機器25から要求された上記提供対象ファイル名および上記アクセス権判定結果を受信し、データ送信部232に送る（ステップS34）。そして、データ送信部232は、上記アクセス権判定結果の正当性をサーバ21によって判定された結果が否か等によって判断する（ステップS35）。このステップS35では、データ送信部232は、上記ステップS30でサーバ21によって暗号化されたアクセス権判定結果を解くことによって、その正当性を確認することができる。そして、データ送信部232は、上記アクセス権判定結果が正当であった場合、第2のクライアント機器25から要求されたデータを、記憶装置制御部233を制御することによってデータ記憶装置24から検索し、当該データをクライアント間通信部231を介して第2のクライアント機器25に送信する（ステップS36）。また、上記ステップS33で複製条件情報も同時に送信されている場合、要求されたデータは、その複製条件情報と共に第2のクライアント機器25に送信される。一方、上記アクセス権判定結果が不当であった場合、第2のクライアント機器25に対するデータ送信を拒否する。

【0116】次に、第2のクライアント機器25のクライアント間通信部254は、上記ステップS36で送信されたデータを受信し、データ受信部256に送る（ステップS37）。そして、データ受信部256は、記憶装置制御部255を制御することによって、上記ステップS37で受信したデータをデータ記憶装置26に格納したり、表示装置257に当該データを表示したりする。また、上記ステップS37で受信したデータが上記複製条件情報と共に受信された場合、当該データは以後の複製に関して、当該複製条件情報に制限される。なお、この複製の制限については、後述する。

【0117】アクセス権管理データベース22に格納されているアクセス権管理リストのデータ構造については、図6を用いて説明した第1の実施形態のデータ構造と同様である。また、上記ステップS29（図13を参照）でアクセス可否判定部211が行うアクセス権判定処理の詳細な動作についても、図7を用いて説明した第1の実施形態のサブルーチンと同様である。つまり、アクセス可否判定部211は、第2の実施形態においても、複数の記述条件で記述されたアクセス権管理リストに対して、その記述条件に応じた動作手順を用いることによって、適切にアクセス可否の判定が可能である。したがって、第2の実施形態において、アクセス権管理リストのデータ構造およびアクセス可否判定部211が行うアクセス権判定処理の詳細な動作についての詳細な説明は省略する。

【0118】なお、第2の実施形態では、第1のクライアント機器23は、上記ステップS23において、自身

をデータ一覧として作成したが、第2のクライアント機器25が第1のクライアント機器23からアクセス可能なデータのみを、サーバ21に問い合わせることによって、サーバ21から上記データ一覧を取得してもかまわない。これは、第2のクライアント機器25が、上記ステップS21でデータ一覧要求をサーバ21に送信することによって、第2のクライアント機器25がアクセス可能なデータ返信するように、アクセス権問い合わせを行う。そして、サーバ21において第2のクライアント機器25がアクセス可能なデータをアクセス権管理リストから検索して上記データ一覧を作成することによって、アクセス可能なデータのみを上記データ一覧として作成し、第2のクライアント機器25に送信することができる。

【0119】また、第2の実施形態の説明では、第2のクライアント機器25の認証に関する手法を記述していないが、サーバ21と第1および第2のクライアント機器23および25との間で、認証によって正しいクライアント機器からの通信であることを確認してもかまわない。つまり、第2のクライアント機器25から第1のクライアント機器23あるいはサーバ21への通信の際には、第2のクライアント機器25であることを証明するための第2のクライアント証明書を送信することによって、サーバ21および第1のクライアント機器23は、この証明書を認証して、正しいクライアント機器からの通信であることを確認することができる。このときに用いられる証明書としては、例えば、電子鍵証明書および証明書失効リストの標準仕様であるX.509等を用いることができる。

【0120】また、サーバ21から第2のクライアント機器25に対して、アクセス権の判定結果と共に複製条件情報が送信される場合、サーバ21は、この複製条件情報に対して所定の暗号化を行う。例えば、サーバ21が所有する秘密鍵で上記複製条件情報に署名して送信することによって、この複製条件が適用されるデータが提供される第2のクライアント機器25に対して正当性が保証される。また、この複製条件が適用されるデータは、DRM(Digital Rights Management)方式で暗号化される。例えば、データの提供元である第1のクライアント機器23では、サーバ21からアクセス権の判定結果と共に複製条件情報が送信された場合、その複製条件情報が適用されるデータに対して第2のクライアント機器25が公開する公開鍵で暗号化し、上記複製条件情報と共に第2のクライアント機器25に送信する。そして、第2のクライアント機器25では、秘密鍵を耐タンパ領域に格納し、当該機器の利用者に対しても秘密になるように保持しておく。これによって、第2のクライアント機器25以外に上記データを不正にコピーした場合でもデータの復号化は不可能

件にしたがってコピーを行う場合には、暗号化されたデータを第2のクライアント機器25の秘密鍵で一度復号化し、再度複製先機器が公開する公開鍵を用いて暗号化することによって、複製を制限することが可能である。なお、ここではデータを直接公開鍵で暗号化するとしたが、データを共通鍵方式の暗号鍵で暗号化し、さらにここで使用した暗号鍵を第2のクライアント機器25が公開する公開鍵を用いて第1のクライアント機器23が暗号化し、暗号化したデータと共に暗号鍵を送信してもかまわない。なお、上記複製条件情報の署名が改竄されている（つまり、サーバ21からの情報ではない）場合、その複製条件情報が適用されるデータに対する複製は不可とされる。

【0121】また、サーバ21と第1および第2のクライアント機器23および25との間で行われる通信の経路に関する秘匿性・耐改竄性については、第2の実施形態では特に手法を記述していないが、秘密鍵方式とセッション鍵とを組み合わせた暗号化方式による暗号化通信を行ってもかまわない。このような暗号化通信としては、SSL(Secure Socket Layer)等を用いることができる。

【0122】このように、第2の実施形態に係るアクセス権制御システムによれば、データの提供先となるクライアント機器からアクセス権を問い合わせることによって、ピアツーピアでのデータ交換を行う際のアクセス権の制御を処理能力の高いサーバ側で行うことになり、複雑なアクセス権制御であっても適切に処理することが可能となる。このような複雑なアクセス権制御を実現しながらも、交換すべきデータそのものは、クライアント機器間で直接送受信することによって、サーバにネットワーク帯域上の負荷をかけることなくデータ交換を行うことが可能である。また、クライアント機器が処理能力の限られた民生機器で構成されている場合でも、上記複雑なアクセス権制御がサーバで処理されるため、処理能力の限られた民生機器によるピアツーピアでのデータ交換に対して、上記複雑なアクセス権制御を付加して容易に行うことが可能である。

【0123】なお、上述した第1および第2の実施形態に係るアクセス権制御システムでは、サーバと直接的に接続されたクライアント機器がサーバにアクセス権の判定を依頼し、その結果を相手のクライアント機器に送信することによって構成されているが、アクセス権の判定を依頼するクライアント機器とサーバとは、直接的に接続されていないてもかまわない。上記サーバが、ピアツーピア型のファイル交換システム内に配置されているクライアント機器と通信可能に接続されていれば、サーバと直接的に通信可能な他のプロキシとしてのクライアント機器（第3のクライアント機器とする）を介して、アクセス権の判定を依頼するクライアント機器とサーバと

えば、上述した第1の実施形態では、第1のクライアント機器13がサーバ11と直接的に通信できない場合、第1のクライアント機器13が上記第3のクライアント機器を介してサーバ11と通信することによって、同様のアクセス権制御システムを構成することが可能である。また、上述した第2の実施形態では、第2のクライアント機器25がサーバ21と直接的に通信できない場合、第2のクライアント機器25が上記第3のクライアント機器を介してサーバ21と通信することによって、同様のアクセス権制御システムを構成することが可能である。このように上記第3のクライアント機器を介してアクセス権制御システムを構成する場合、さらに第3のクライアント機器であることを証明するための第3のクライアント証明書を用いて、それぞれのクライアント機器およびサーバが互いに認証することによって、正しいクライアント機器からの通信であることを確認することができることは、言うまでもない。

【図面の簡単な説明】

【図1】本発明の第1の実施形態に係るアクセス権制御システムの全体の構成について説明するための図である。

【図2】図1に示すサーバ11の内部構成を示す機能ブロック図である。

【図3】図1に示す第1のクライアント機器13の内部構成を示す機能ブロック図である。

【図4】図1に示す第2のクライアント機器15の内部構成を示す機能ブロック図である。

【図5】図1に示すサーバ11、第1および第2のクライアント機器13および15が処理する全体動作を示すフローチャートである。

【図6】図1に示すアクセス権管理データベース12に格納されているアクセス権管理リストのデータ構造について説明する図である。

【図7】図5に示すステップS11において、アクセス可否判定部111が行うアクセス権判定処理の詳細動作

の一例を示すサブルーチンである。

【図8】図5に示すステップS11において、アクセス可否判定部111が行うアクセス権判定処理の詳細動作の他の例を示すサブルーチンである。

【図9】本発明の第2の実施形態に係るアクセス権制御システムの全体の構成について説明するための図である。

【図10】図9に示すサーバ21の内部構成を示す機能ブロック図である。

【図11】図9に示す第1のクライアント機器23の内部構成を示す機能ブロック図である。

【図12】図9に示す第2のクライアント機器25の内部構成を示す機能ブロック図である。

【図13】図9に示すサーバ21、第1および第2のクライアント機器23および25が処理する全体動作を示すフローチャートである。

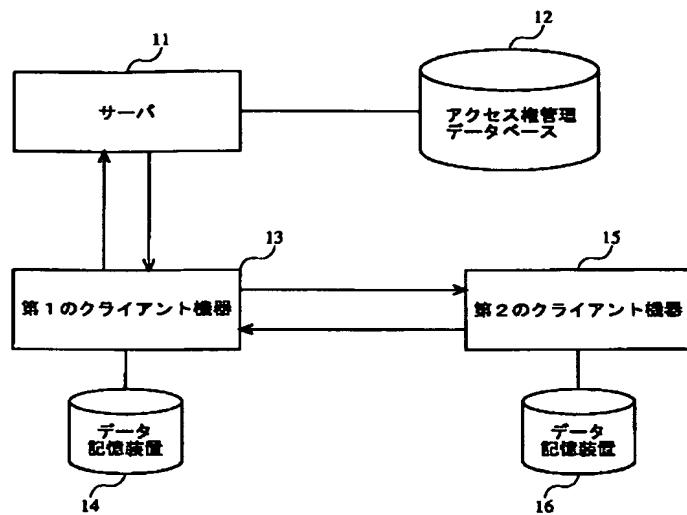
【符号の説明】

- 11、21…サーバ
- 12、22…アクセス権管理データベース
- 13、23…第1のクライアント機器
- 14、16、24、26…データ記憶装置
- 15、25…第2のクライアント機器
- 111、211…アクセス可否判定部
- 112、212…データベース制御部
- 113、134、151、213、231、254…クライアント間通信部
- 131、251…サーバ間通信部
- 132、252…アクセス可否問い合わせ部
- 133、132…データ送信部
- 135、154、233、255…記憶装置制御部
- 152、253…データ要求部
- 153、256…データ受信部
- 155、257…表示装置
- 156、258…入力装置

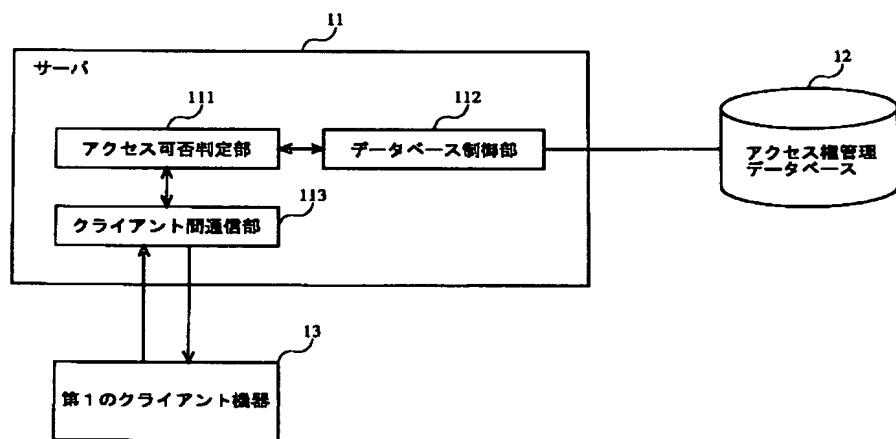
【図6】

番号	提供元識別子	ファイル名	提供先識別子	時間条件	回数条件	複製条件
1	1111	慶声.wav	2222	任意	任意	不可
2	1111	誕生.jpg	任意	2001/03/31まで	任意	不可
3	1111	誕生金.mov	3333	任意	2回	任意
4	1111	子供.jpg	2222, 3333	2001/07/31まで	任意	1世代のみ可
5	1111	お祝い金.txt	1111, 4444	任意	任意	任意
6	2222	海外旅行.mov	1111	2001/06/01から1ヶ月	1回	任意
7	2222	連絡事項.txt	1111, 2222	任意	任意	不可
8	3333	結婚式.mov	任意	2001/07/31まで	任意	不可
9	4444	任意	1111	任意	任意	任意
10						
11	:	:	:	:	:	:
12						
13						

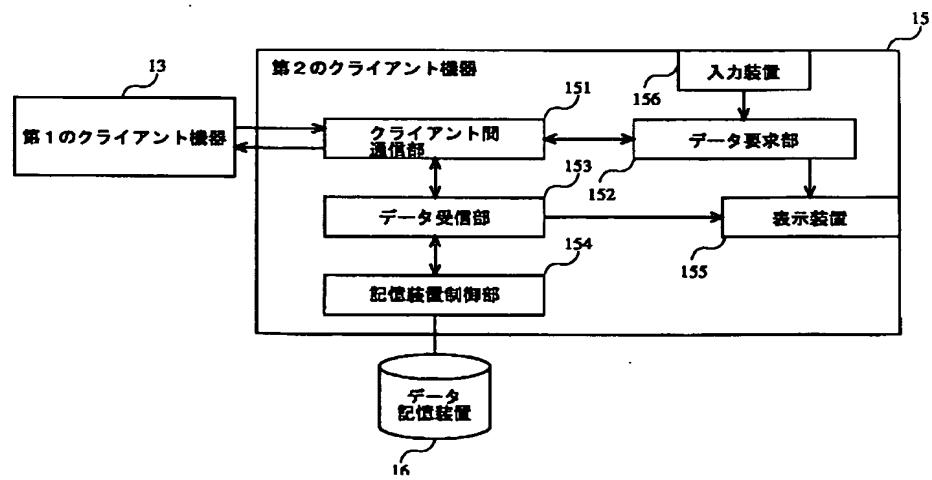
【図1】



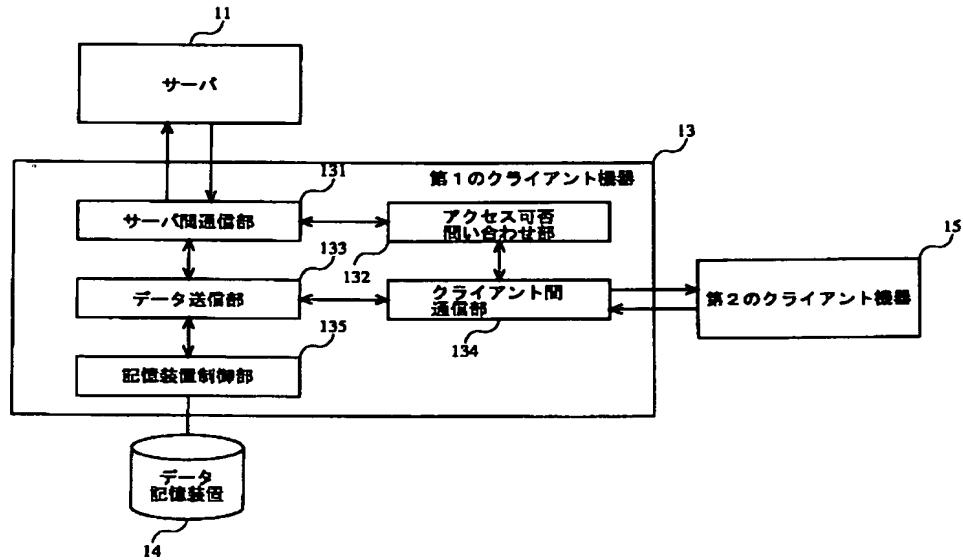
【図2】



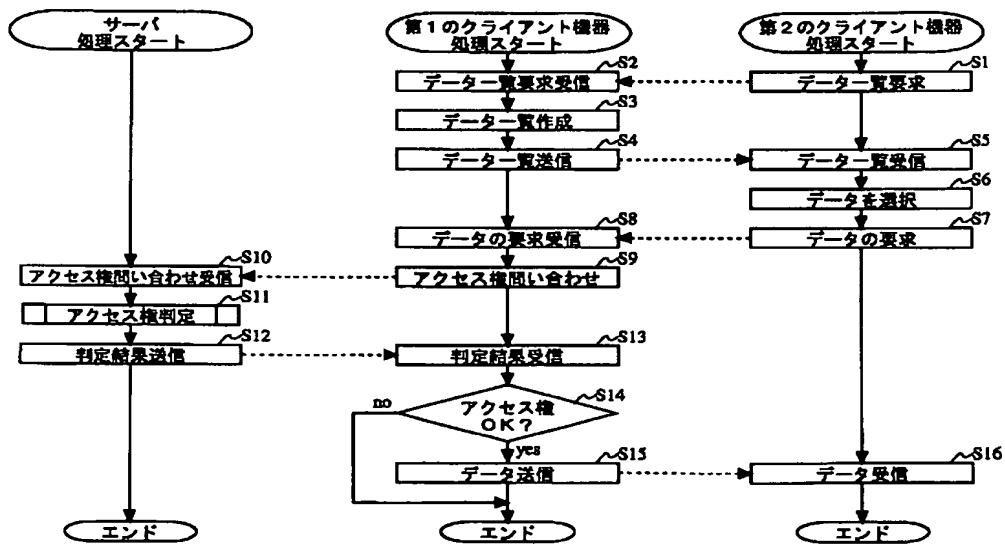
【図4】



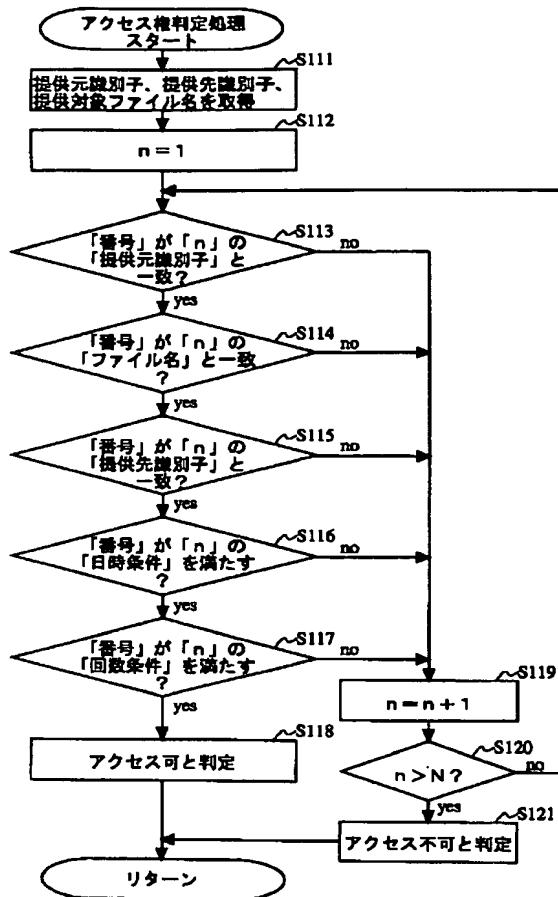
【図3】



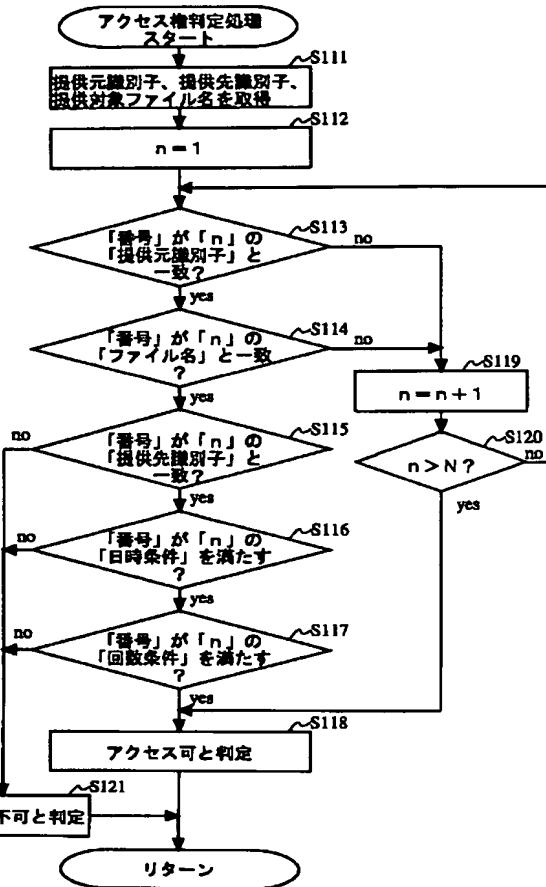
【図5】



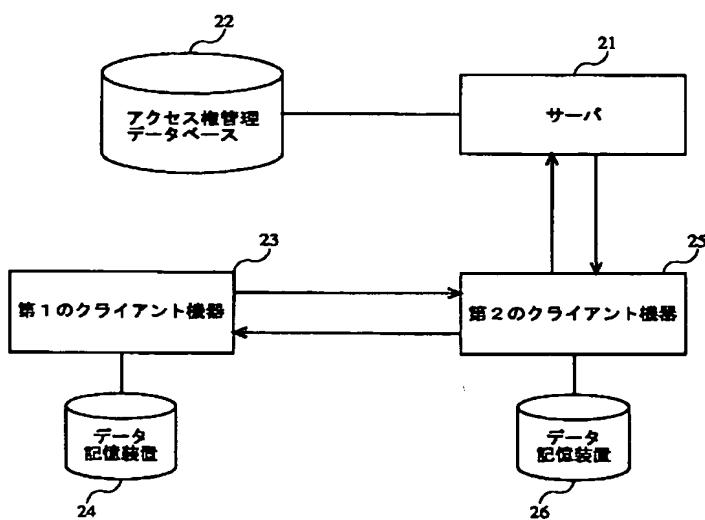
【図7】



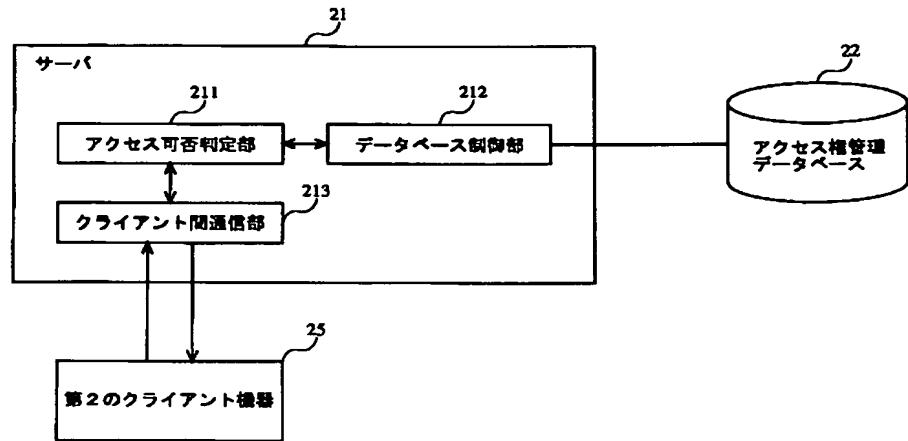
【図8】



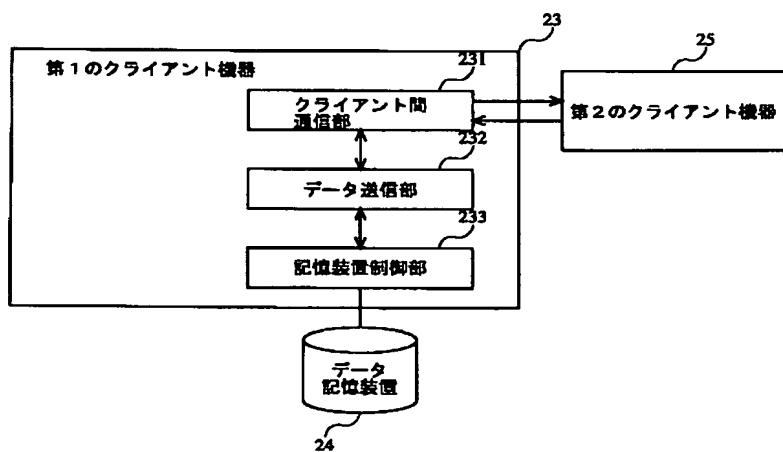
【図9】



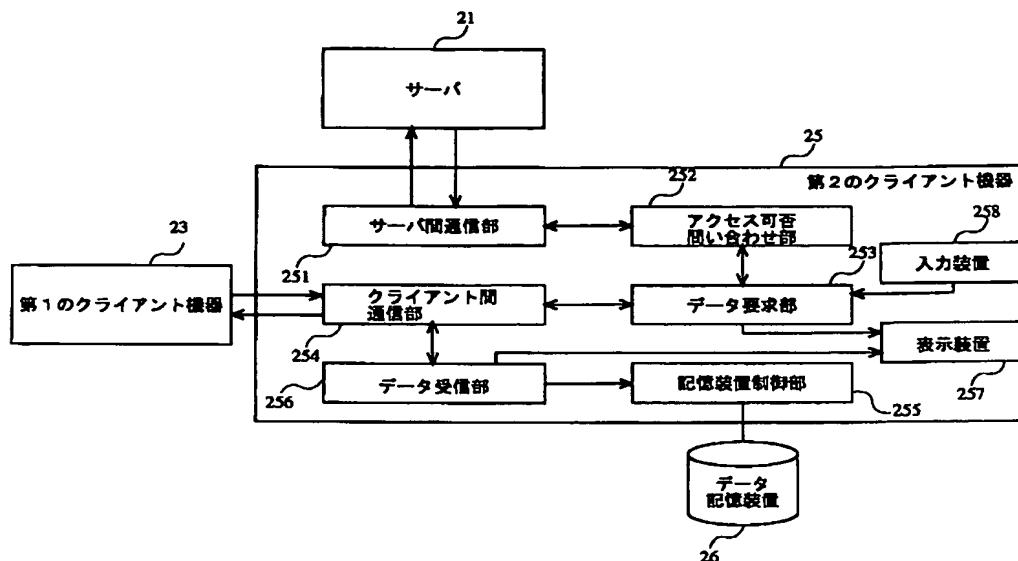
【図10】



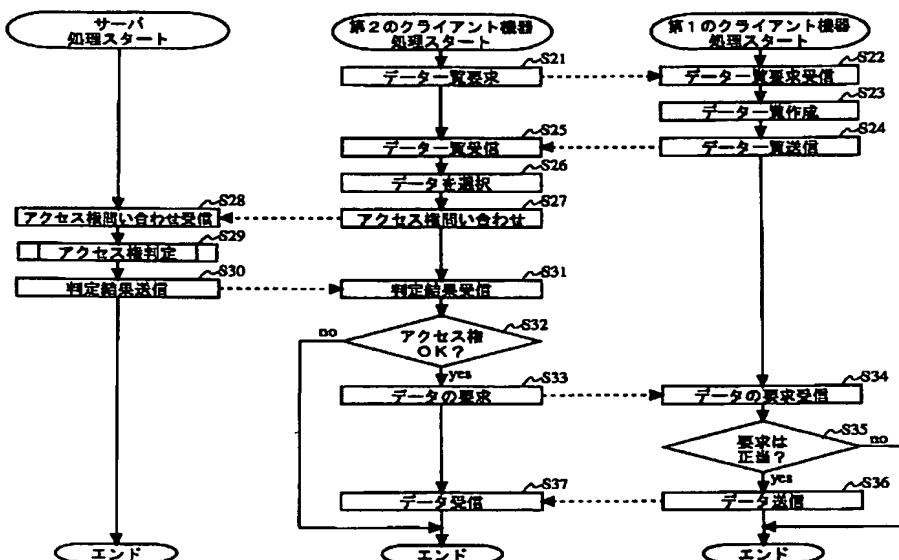
【図11】



【図12】



【図13】



フロントページの続き

(72) 発明者 大穂 雅博

大阪府門真市大字門真1006番地 松下電器
産業株式会社内

F ターム(参考) 5B017 AA07 BA06 BB06 CA16

5B082 EA11

5B085 AE04 AE23 BA07 BE01 BE04

BG02 BG07